CDP Public Cloud 7.2.16

Cloudera Manager Configuration Properties

Date published: 2019-11-22
Date modified: 2023-03-20

CLOUDERA

https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2025. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Cloudera Manager 7.12.0 Configuration Properties.....10

Cloudera Manager Configuration Properties Reference for Cloudera Runtime 7.2.18.....10

ADLS Connector Properties in Cloudera Runtime 7.2.18.....10
Service-Wide.....10
Atlas Properties in Cloudera Runtime 7.2.18.....12
Atlas Server.....12
Gateway.....66
Service-Wide.....69
Core Configuration Properties in Cloudera Runtime 7.2.18.....94
Gateway.....94
Service-Wide.....97
Cruise Control Properties in Cloudera Runtime 7.2.18.....137
Cruise Control Server.....137
Service-Wide.....180
Data Analytics Studio Properties in Cloudera Runtime 7.2.18.....197
Data Analytics Studio Eventprocessor.....197
Data Analytics Studio Webapp Server.....224
Service-Wide.....266
Data Context Connector Properties in Cloudera Runtime 7.2.18.....293
Gateway.....293
Service-Wide.....298
Flink Properties in Cloudera Runtime 7.2.18.....301
Flink Dashboard.....301
Gateway.....324
Service-Wide.....329
GCS Properties in Cloudera Runtime 7.2.18.....360
Service-Wide.....360
HBase Properties in Cloudera Runtime 7.2.18.....361
Gateway.....361
HBase REST Server.....367
HBase Thrift Server.....401
Master.....434
RegionServer.....474
Service-Wide.....532
HDFS Properties in Cloudera Runtime 7.2.18.....605
Balancer.....605
DataNode.....614
Failover Controller.....658
Gateway.....686
HttpFS.....691
JournalNode.....725
NameNode.....759
NFS Gateway.....817
SecondaryNameNode.....850
Service-Wide.....883
Hive Properties in Cloudera Runtime 7.2.18.....967

Gateway....967
Hive Metastore Server....972
HiveServer2....1007
Service-Wide....1061
WebHCat Server....1128
Hive LLAP Properties in Cloudera Runtime in 7.2.18....1156
Gateway....1156
HiveServer2....1160
LLAP Proxy....1227
Service-Wide....1263
Hive on Tez Properties in Cloudera Runtime 7.2.18....1314
Gateway....1314
HiveServer2....1319
Service-Wide....1374
Hue Properties in Cloudera Runtime 7.2.18....1427
Hue Server....1427
Kerberos Ticket Renewer....1456
Load Balancer....1475
Service-Wide....1499
Iceberg Replication Properties in Cloudera Runtime 7.2.18....1542
Admin Server....1542
Service-Wide....1566
Impala Properties in Cloudera Runtime 7.2.18....1581
Impala Catalog Server....1581
Impala Daemon....1619
Impala StateStore....1682
Service-Wide....1713
Java KeyStore KMS Properties in Cloudera Runtime 7.2.18....1773
Key Management Server....1773
Service-Wide....1815
Kafka Properties in Cloudera Runtime 7.2.18....1832
Gateway....1832
Kafka Broker....1836
Kafka Connect....1890
Kafka MirrorMaker....1929
Service-Wide....1970
Key Trustee Server Properties in Cloudera Runtime 7.2.18....2024
Active Database....2024
Active Key Trustee Server....2041
Passive Database....2064
Passive Key Trustee Server....2082
Service-Wide....2105
Key-Value Store Indexer Properties in Cloudera Runtime 7.2.18....2120
Lily HBase Indexer....2120
Service-Wide....2147
Knox Properties in Cloudera Runtime 7.2.18....2162
Gateway....2162
Knox Gateway....2164
Knox IDBroker....2227
Service-Wide....2276
Kudu Properties in Cloudera Runtime 7.2.18....2313
Master....2313
Service-Wide....2341
Tablet Server....2363
Livy Properties in Cloudera Runtime 7.2.18....2388
Gateway....2388

Livy Server ... 2391
Service-Wide ... 2421
Oozie Properties in Cloudera Runtime 7.2.18 ... 2435
Oozie Server ... 2435
Service-Wide ... 2482
Ozone Properties in Cloudera Runtime 7.2.18 ... 2507
Gateway ... 2508
HttpFS Gateway ... 2513
Ozone DataNode ... 2547
Ozone Manager ... 2585
Ozone Prometheus ... 2629
Ozone Recon ... 2652
S3 Gateway ... 2688
Service-Wide ... 2721
Storage Container Manager ... 2779
Phoenix Properties in Cloudera Runtime 7.2.18 ... 2831
Query Server ... 2831
Service-Wide ... 2859
Ranger Properties in Cloudera Runtime 7.2.18 ... 2872
Ranger Admin ... 2872
Ranger Tagsync ... 2922
Ranger Usersync ... 2955
Service-Wide ... 3001
Ranger KMS Properties in Cloudera Runtime 7.2.18 ... 3039
Ranger KMS Server ... 3039
Service-Wide ... 3101
Ranger KMS with Key Trustee Server Properties in Cloudera Runtime 7.2.18 ... 3131
Ranger KMS Server with KTS ... 3132
Service-Wide ... 3189
Ranger Raz Properties in Cloudera Runtime 7.2.18 ... 3215
Ranger Raz Server ... 3215
Service-Wide ... 3257
Ranger RMS Properties in Cloudera Runtime 7.2.18 ... 3277
Ranger RMS Server ... 3278
Service-Wide ... 3316
S3 Connector Properties in Cloudera Runtime 7.2.18 ... 3333
Service-Wide ... 3333
Schema Registry Properties in Cloudera Runtime 7.2.18 ... 3335
Gateway ... 3335
Schema Registry Server ... 3337
Service-Wide ... 3384
Solr Properties in Cloudera Runtime 7.2.18 ... 3411
Gateway ... 3411
Service-Wide ... 3413
Solr Server ... 3441
Spark Properties in Cloudera Runtime 7.2.18 ... 3476
Gateway ... 3477
History Server ... 3486
Service-Wide ... 3517
SQL Stream Builder Properties in Cloudera Runtime 7.2.18 ... 3535
Materialized View Engine ... 3536
Service-Wide ... 3561
Streaming SQL Console ... 3590
Streaming SQL Engine ... 3625
SQOOP_CLIENT Properties in Cloudera Runtime 7.2.18 ... 3646
Gateway ... 3646

Service-Wide....3651
Streams Messaging Manager Properties in Cloudera Runtime 7.2.18....3656
Service-Wide....3656
Streams Messaging Manager Rest Admin Server....3694
Streams Messaging Manager UI Server....3753
Streams Replication Manager Properties in Cloudera Runtime 7.2.18....3776
Gateway....3776
Service-Wide....3783
SRM Driver....3810
SRM Service....3838
Stub DFS Properties in Cloudera Runtime 7.2.18....3870
Gateway....3870
Service-Wide....3874
Storage Operations....3883
Tez Properties in Cloudera Runtime 7.2.18....3901
Gateway....3902
Service-Wide....3904
YARN Properties in Cloudera Runtime 7.2.18....3926
Gateway....3926
JobHistory Server....3951
NodeManager....3987
ResourceManager....4055
Service-Wide....4101
YARN Queue Manager Properties in Cloudera Runtime 7.2.18....4176
Service-Wide....4176
YARN Queue Manager Store....4192
YARN Queue Manager Webapp....4221
Zeppelin Properties in Cloudera Runtime 7.2.18....4254
Service-Wide....4255
Zeppelin Server....4274
ZooKeeper Properties in Cloudera Runtime 7.2.18....4314
Server....4314
Service-Wide....4359

Host Configuration Properties....4384
Advanced....4384
Monitoring....4386
Parcels....4394
Resource Management....4394
Suppressions....4395

Cloudera Manager Server Properties....4403
Advanced....4403
Altus....4407
Custom Service Descriptors....4407
External Authentication....4408
Kerberos....4419
Monitoring....4427
Network....4428
Other....4430
Parcels....4433
Performance....4438
Ports and Addresses....4439
Replication....4440

Reports....4441
Security....4442
Support....4449
Suppressions....4454

Cloudera Management Service....4480
Activity Monitor - Unsupported Since 7.0.0....4480
Advanced....4480
Database....4484
Logs....4485
Monitoring....4486
Other....4498
Performance....4500
Ports and Addresses....4501
Resource Management....4502
Security....4504
Stacks Collection....4505
Suppressions....4506
Alert Publisher....4519
Advanced....4519
Logs....4523
Monitoring....4524
Other....4533
Performance....4539
Ports and Addresses....4539
Resource Management....4540
SNMP....4542
Stacks Collection....4545
Suppressions....4546
Event Server....4559
Advanced....4559
Logs....4564
Monitoring....4565
Other....4577
Performance....4579
Ports and Addresses....4579
Resource Management....4580
Stacks Collection....4582
Suppressions....4583
Host Monitor....4595
Advanced....4595
Logs....4599
Monitoring....4600
Other....4612
Performance....4614
Ports and Addresses....4615
Resource Management....4616
Security....4618
Stacks Collection....4619
Suppressions....4620
Navigator Audit Server....4633
Advanced....4633
Database....4637
Logs....4639
Monitoring....4640

Other....4650
Performance....4651
Ports and Addresses....4651
Publishing....4651
Resource Management....4652
Security....4654
Stacks Collection....4656
Suppressions....4657
Navigator Metadata Server....4671
Advanced....4671
Cloudera Navigator....4675
Database....4676
External Authentication....4677
Extractor Filter....4686
Logs....4687
Monitoring....4689
Other....4701
Performance....4701
Policies....4702
Ports and Addresses....4703
Resource Management....4703
Security....4705
Stacks Collection....4707
Suppressions....4708
Reports Manager....4731
Advanced....4731
Database....4735
Logs....4737
Monitoring....4738
Other....4749
Performance....4750
Ports and Addresses....4750
Resource Management....4751
Security....4753
Stacks Collection....4753
Suppressions....4755
Service Monitor....4767
Advanced....4767
Logs....4771
Monitoring....4772
Other....4786
Performance....4791
Ports and Addresses....4792
Resource Management....4793
Security....4795
Stacks Collection....4797
Suppressions....4798
Service-Wide....4813
Advanced....4813
Monitoring....4815
Other....4823
Publishing....4824
Security....4824
Suppressions....4825
Telemetry Publisher....4876
Advanced....4876

Logs....4882
Monitoring....4883
Other....4895
Performance....4895
Ports and Addresses....4896
Resource Management....4896
Security....4898
Stacks Collection....4900
Suppressions....4901

Cloudera Manager 7.12.0 Configuration Properties

This guide provides reference information on configuration properties supported by Cloudera Manager 7.12.0. Available properties may differ by Cloudera Runtime version.

Cloudera Manager Configuration Properties Reference for Cloudera Runtime 7.2.18

Refer to the following links for a list of available Cloudera Runtime configuration properties available in Cloudera Manager 7.12.0 to manage Cloudera Runtime 7.2.18.

This section provides reference information on configuration properties supported by Cloudera Manager 7.12.0 to manage Cloudera Runtime 7.2.18.

ADLS Connector Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

ADLS Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ADLS_CONNECTOR_service_env_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Cloud Account Name

Description

Name of an Azure account. The associated keys are emitted to Hue, Impala and the Hive Metastore Server.

Related Name

Default Value

API Name

cloud_account

Required

true

Hue Browser Data Lake Store

Description

This is required only for clusters using Hue with ADLS Gen1. Determines the Data Lake Store for the Hue browser. This is usually of the form: yourstorename.azuredatalakestore.net.

Related Name

Default Value

API Name

hue_browser_dls

Required

false

Credentials Protection Policy

Description

Determines a security policy for the distribution of Azure account credentials to cluster services. 'More Secure': Encrypted at all times and directly available to a limited set of services. 'Less Secure': Credentials may be in plain text in some configuration files for specific services in the cluster.

Related Name

Default Value

SECURE

API Name

key_distribution_policy

Required

true

Suppressions

Suppress Parameter Validation: ADLS Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ADLS Connector Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_adls_connector_service_env_safety_valve

Required

true

Suppress Parameter Validation: Hue Browser Data Lake Store

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Browser Data Lake Store parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_browser_dls

Required

true

Suppress Configuration Validator: ADLS Hue Browser DLS required validator

Description

Whether to suppress configuration warnings produced by the ADLS Hue Browser DLS required validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_browser_dls_required_validator

Required

true

Atlas Properties in Cloudera Runtime 7.2.18

Role groups:

Atlas Server

Advanced

Atlas Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

ATLAS_SERVER_role_env_safety_valve

Required

false

Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

For advanced use only. A string to be inserted into conf/atlas-application.properties for this role only.

Related Name

Default Value

API Name

conf/atlas-application.properties_role_safety_valve

Required

false

Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-audit.xml

Description

For advanced use only. A string to be inserted into conf/ranger-atlas-audit.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-atlas-audit.xml_role_safety_valve

Required

false

Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-atlas-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-atlas-policymgr-ssl.xml_role_safety_valve

Required

false

Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-security.xml

Description

For advanced use only. A string to be inserted into conf/ranger-atlas-security.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-atlas-security.xml_role_safety_valve

Required

false

Atlas Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Atlas Server Log Directory

Description

The log directory for log files of the role Atlas Server.

Related Name

atlas.log.base.dir

Default Value

/var/log/atlas

API Name

log_dir

Required

false

Atlas Server Logging Threshold

Description

The minimum log level for Atlas Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Atlas Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Atlas Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Atlas Server Max Log Size

Description

The maximum size, in megabytes, per log file for Atlas Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

atlas_server_fd_thresholds

Required

false

Atlas Server Host Health Test

Description

When computing the overall Atlas Server health, consider the host's health.

Related Name

Default Value

true

API Name

atlas_server_host_health_enabled

Required

false

Atlas Server Process Health Test

Description

Enables the health test that the Atlas Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

atlas_server_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Admin Password

Description

Password for the Atlas Admin user configured in property atlas.admin.username with default value named "admin". Password should be minimum 8 characters with minimum one alphabet and one numeric. Unsupported special characters are " ' \ ` ´.

Related Name

atlas.admin.password

Default Value

API Name

atlas_admin_password

Required

false

Admin Username

Description

Admin Login user.

Related Name

atlas.admin.username

Default Value

admin

API Name

atlas_admin_username

Required

false

Audit ZooKeeper Session Timeout

Description

Audit ZooKeeper Session Timeout

Related Name

atlas.audit.zookeeper.session.timeout.ms

Default Value

1 minute(s)

API Name

atlas_audit_zookeeper_session_timeout_ms

Required

false

Enable File Authentication

Description

Whether file-based authentication is enabled.

Related Name

atlas.authentication.method.file

Default Value

false

API Name

atlas_authentication_method_file

Required

false

Path to Credentials for File-based Login.

Description

Path to Credentials for File-based Login

Related Name

atlas.authentication.method.file.filename

Default Value

ATLAS_USER_CREDENTIALS_CONF_PATH/users-credentials.properties

API Name

atlas_authentication_method_file_filename

Required

false

Enable LDAP Authentication

Description

Whether LDAP is used for authentication.

Related Name

atlas.authentication.method.ldap

Default Value

false

API Name

atlas_authentication_method_ldap

Required

false

AD Base DN

Description

The Distinguished Name (DN) of the starting point for directory server searches.

Related Name

atlas.authentication.method.ldap.ad.base.dn

Default Value

API Name

atlas_authentication_method_ldap_ad_base_dn

Required

false

AD Bind DN Username

Description

Full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search.

Related Name

atlas.authentication.method.ldap.ad.bind.dn

Default Value

API Name

atlas_authentication_method_ldap_ad_bind_dn

Required

false

AD Bind DN Password

Description

Password for the account that can search

Related Name

atlas.authentication.method.ldap.ad.bind.password

Default Value

API Name

atlas_authentication_method_ldap_ad_bind_password

Required

false

AD User Default Role

Description

AD User default Role

Related Name

atlas.authentication.method.ldap.ad.default.role

Default Value

ROLE_USER

API Name

atlas_authentication_method_ldap_ad_default_role

Required

false

AD Domain Name (Only for AD)

Description

AD domain, only used if Authentication method is AD

Related Name

atlas.authentication.method.ldap.ad.domain

Default Value

API Name

atlas_authentication_method_ldap_ad_domain

Required

false

AD Referral

Description

This parameter is only used if Authentication method is AD. Set to follow if multiple ADsss servers are configured to return continuation references for results. Set to ignore (default) if no referrals should be followed. When this parameter is set to throw, all of the normal entries are returned in the enumeration first, before the ReferralException is thrown.

Related Name

atlas.authentication.method.ldap.ad.referral

Default Value

ignore

API Name

atlas_authentication_method_ldap_ad_referral

Required

false

AD URL

Description

AD URL, only used if Authentication method is AD

Related Name

atlas.authentication.method.ldap.ad.url

Default Value

API Name

atlas_authentication_method_ldap_ad_url

Required

false

AD User Search Filter

Description

AD User Search Filter

Related Name

atlas.authentication.method.ldap.ad.user.searchfilter

Default Value

(sAMAccountName=0)

API Name

atlas_authentication_method_ldap_ad_user_searchfilter

Required

false

LDAP DN

Description

The Distinguished Name (DN) of the starting point for directory server searches.

Related Name

atlas.authentication.method.ldap.base.dn

Default Value

API Name

atlas_authentication_method_ldap_base_dn

Required

false

LDAP Bind DN Username

Description

Full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search.

Related Name

atlas.authentication.method.ldap.bind.dn

Default Value

API Name

atlas_authentication_method_ldap_bind_dn

Required

false

LDAP Bind DN Password

Description

Password for the account that can search in LDAP

Related Name

atlas.authentication.method.ldap.bind.password

Default Value

API Name

atlas_authentication_method_ldap_bind_password

Required

false

LDAP User Default Role

Description

LDAP User Default Role

Related Name

atlas.authentication.method.ldap.default.role

Default Value

ROLE_USER

API Name

atlas_authentication_method_ldap_default_role

Required

false

LDAP Group-Role Attribute

Description

LDAP Group-Role Attribute

Related Name

atlas.authentication.method.ldap.groupRoleAttribute

Default Value

cn

API Name

atlas_authentication_method_ldap_groupRoleAttribute

Required

false

LDAP Group-Search Base

Description

LDAP Group-Search Base

Related Name

atlas.authentication.method.ldap.groupSearchBase

Default Value

API Name

atlas_authentication_method_ldap_groupSearchBase

Required

false

LDAP Group-Search Filter

Description

LDAP Group-Search Filter

Related Name

atlas.authentication.method.ldap.groupSearchFilter

Default Value

API Name

atlas_authentication_method_ldap_groupSearchFilter

Required

false

LDAP Referral

Description

This parameter is only used if Authentication method is LDAP. Set to follow if multiple LDAP servers are configured to return continuation references for results. Set to ignore (default) if no referrals should be followed. When this parameter is set to throw, all of the normal entries are returned in the enumeration first, before the ReferralException is thrown.

Related Name

atlas.authentication.method.ldap.referral

Default Value

ignore

API Name

atlas_authentication_method_ldap_referral

Required

false

LDAP Authentication Type

Description

The LDAP type (ldap, ad, or none).

Related Name

atlas.authentication.method.ldap.type

Default Value

none

API Name

atlas_authentication_method_ldap_type

Required

false

LDAP UGI Groups

Description

LDAP UGI Groups

Related Name

atlas.authentication.method.ldap.ugi-groups

Default Value

false

API Name

atlas_authentication_method_ldap_ugi_groups

Required

false

LDAP Server URL

Description

LDAP Server URL. Sample values = ldap://localhost:389 or ldaps://localhost:636

Related Name

atlas.authentication.method.ldap.url

Default Value

API Name

atlas_authentication_method_ldap_url

Required

false

LDAP User Search Filter

Description

LDAP User Search Filter

Related Name

atlas.authentication.method.ldap.user.searchfilter

Default Value

API Name

atlas_authentication_method_ldap_user_searchfilter

Required

false

User DN Pattern

Description

User DN Pattern. This pattern is used to create a distinguished name (DN) for a user during login

Related Name

atlas.authentication.method.ldap.userDNpattern

Default Value

uid=

API Name

atlas_authentication_method_ldap_userDNpattern

Required

false

Enable PAM Authentication

Description

Whether PAM is used for authentication.

Related Name

atlas.authentication.method.pam

Default Value

true

API Name

atlas_authentication_method_pam

Required

false

Enable Knox Trusted Proxy Support

Description

Determine if the Atlas service should allow authentication using Knox trusted proxy.

Related Name

atlas.authentication.method.trustedproxy

Default Value

true

API Name

atlas_authentication_method_trustedproxy

Required

false

Kafka Zookeeper Connection Timeout

Description

Kafka Zookeeper Connection Timeout

Related Name

atlas.kafka.zookeeper.connection.timeout.ms

Default Value

30 second(s)

API Name

atlas_kafka_zookeeper_connection_timeout_ms

Required

false

Kafka ZooKeeper Session Timeout

Description

Kafka ZooKeeper Session Timeout

Related Name

atlas.kafka.zookeeper.session.timeout.ms

Default Value

1 minute(s)

API Name

atlas_kafka_zookeeper_session_timeout_ms

Required

false

Kafka ZooKeeper Sync Time

Description

Kafka ZooKeeper Sync Time

Related Name

atlas.kafka.zookeeper.sync.time.ms

Default Value

20 millisecond(s)

API Name

atlas_kafka_zookeeper_sync_time_ms

Required

false

Atlas Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

atlas_max_heap_size

Default Value

2 GiB

API Name

atlas_max_heap_size

Required

true

Knox Proxy User Groups

Description

Accepts a list of group names. The Knox user can impersonate only the users that belong to the groups specified in the list. The wildcard value * may be used to allow impersonation of any user belonging to any group.

Related Name

atlas.proxyuser.knox.groups

Default Value

*

API Name

atlas_proxyuser_knox_groups

Required

false

Knox Proxy User Hosts

Description

Accepts a list of IP addresses, IP addressranges in CIDR format and/or host names. The Knox user can impersonate only the requests coming from hosts specified in the list. The wildcard value * may be used to allow impersonation from any host.

Related Name

atlas.proxyuser.knox.hosts

Default Value

*

API Name

atlas_proxyuser_knox_hosts

Required

false

Knox Proxy User Users

Description

Accepts a list of usernames. The Knox user can impersonate only the users specified in the list. The wildcard value * may be used to allow impersonation of any user.

Related Name

atlas.proxyuser.knox.users

Default Value

*

API Name

atlas_proxyuser_knox_users

Required

false

Proxy Users

Description

Atlas service can be proxied through Knox, hence need to configure the proxy users using which Atlas service can be proxied

Related Name

atlas.proxyusers

Default Value

API Name

atlas_proxyusers

Required

false

Server Bind Address

Description

The Server will bind to this address.

Related Name

atlas.server.bind.address

Default Value

0.0.0.0

API Name

atlas_server_bind_address

Required

false

Simple Authz policy file

Description

Path for the Simple Authz Policies File.

Related Name

atlas.simple.authz.policy.file

Default Value

ATLAS_SIMPLE_AUTHZ_POLICY_CONF_PATH/atlas-simple-authz-policy.json

API Name

atlas_simple_authz_policy_file

Required

false

Initial Solr Replication Factor for Collections

Description

Solr Replication Factor for Collections. This only affects the initial setting and has no effect once Atlas has started for the first time.

Related Name

atlas_solr_replication_factor

Default Value

1

API Name

atlas_solr_replication_factor

Required

false

Initial Solr Shards for Atlas Collections

Description

Solr Shards for Collections. This only affects the initial setting and has no effect once Atlas has started for the first time.

Related Name

atlas_solr_shards

Default Value

1

API Name

atlas_solr_shards

Required

false

Excluded Wire Encryption Protocols

Description

A comma-separated list of the wire encryption protocols to exclude when TLS is enabled. Some versions of cURL do not work with TLSv1.2.

Related Name

atlas.ssl.exclude.protocols

Default Value

TLSv1.2

API Name

atlas_ssl_exclude_protocols

Required

false

Knox SSO browser User-Agent

Description

Knox SSO browser User-Agent

Related Name

atlas.sso.knox.browser.useragent

Default Value

API Name

atlas_sso_knox_browser_useragent

Required

false

Enable Knox SSO

Description

Enable Knox SSO

Related Name

atlas.sso.knox.enabled

Default Value

false

API Name

atlas_sso_knox_enabled

Required

false

Knox SSO provider URL

Description

Knox SSO provider URL.

Related Name

atlas.sso.knox.providerurl

Default Value

API Name

atlas_sso_knox_providerurl

Required

false

Knox SSO Public-Key

Description

Knox SSO Public-Key

Related Name

atlas.sso.knox.publicKey

Default Value

API Name

atlas_sso_knox_publicKey

Required

false

Atlas Server Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Kafka Message Retention Time

Description

The maximum time for retaining Kafka messages for topic ATLAS_HOOK. If set to -1, no time limit will be applied. This configuration will be only effective for pre-start initialization of Atlas service and ineffective once the ATLAS_HOOK topic is created for Atlas.

Related Name

retention.ms

Default Value

31 day(s)

API Name

kafka_message_retention_ms

Required

false

Ranger Atlas Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/atlas/audit/hdfs/spool

API Name

ranger_atlas_plugin_hdfs_audit_spool_directory

Required

true

Ranger Atlas Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.atlas.policy.cache.dir

Default Value

/var/lib/ranger/atlas/policy-cache

API Name

ranger_atlas_plugin_policy_cache_directory

Required

true

Ranger Atlas Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/atlas/audit/solr/spool

API Name

ranger_atlas_plugin_solr_audit_spool_directory

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.atlas.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.atlas.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Server HTTP port

Description

Server HTTP port

Related Name

atlas.server.http.port

Default Value

31000

API Name

atlas_server_http_port

Required

false

Server HTTPS Port

Description

Server HTTPS Port

Related Name

atlas.server.https.port

Default Value

31443

API Name

atlas_server_https_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Atlas Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Atlas Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

truststore.file

Default Value

API Name

ssl_client_truststore_location

Required

false

Atlas Server TLS/SSL Trust Store Password

Description

The password for the Atlas Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Atlas Server

Description

Encrypt communication between clients and Atlas Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

atlas.enableTLS

Default Value

false

API Name

ssl_enabled

Required

false

Atlas Server TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Atlas Server is acting as a TLS/SSL server.

Related Name

password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Atlas Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Atlas Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Atlas Server TLS/SSL Server Keystore File Password

Description

The password for the Atlas Server keystore file.

Related Name

keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Admin Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_admin_password

Required

true

Suppress Parameter Validation: Admin Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_admin_username

Required

true

Suppress Parameter Validation: Path to Credentials for File-based Login.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to Credentials for File-based Login. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_file_filename

Required

true

Suppress Parameter Validation: AD Base DN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD Base DN parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_base_dn

Required

true

Suppress Parameter Validation: AD Bind DN Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD Bind DN Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_bind_dn

Required

true

Suppress Parameter Validation: AD Bind DN Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD Bind DN Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_bind_password

Required

true

Suppress Parameter Validation: AD User Default Role

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD User Default Role parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_default_role

Required

true

Suppress Parameter Validation: AD Domain Name (Only for AD)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD Domain Name (Only for AD) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_domain

Required

true

Suppress Parameter Validation: AD URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_url

Required

true

Suppress Parameter Validation: AD User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AD User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_user_searchfilter

Required

true

Suppress Parameter Validation: LDAP DN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP DN parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_base_dn

Required

true

Suppress Parameter Validation: LDAP Bind DN Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind DN Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_bind_dn

Required

true

Suppress Parameter Validation: LDAP Bind DN Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind DN Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_bind_password

Required

true

Suppress Parameter Validation: LDAP User Default Role

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Default Role parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_default_role

Required

true

Suppress Parameter Validation: LDAP Group-Role Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group-Role Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_grouproleattribute

Required

true

Suppress Parameter Validation: LDAP Group-Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group-Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_groupsearchbase

Required

true

Suppress Parameter Validation: LDAP Group-Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group-Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_groupsearchfilter

Required

true

Suppress Parameter Validation: LDAP Server URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Server URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_url

Required

true

Suppress Parameter Validation: LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_user_searchfilter

Required

true

Suppress Parameter Validation: User DN Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the User DN Pattern parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_userdnpattern

Required

true

Suppress Parameter Validation: Atlas Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_max_heap_size

Required

true

Suppress Parameter Validation: Knox Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_groups

Required

true

Suppress Parameter Validation: Knox Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_hosts

Required

true

Suppress Parameter Validation: Knox Proxy User Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_users

Required

true

Suppress Parameter Validation: Proxy Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyusers

Required

true

Suppress Parameter Validation: Server Bind Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server Bind Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_bind_address

Required

true

Suppress Parameter Validation: Server HTTP port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server HTTP port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_http_port

Required

true

Suppress Parameter Validation: Server HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_https_port

Required

true

Suppress Parameter Validation: Atlas Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Simple Authz policy file

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Simple Authz policy file parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_simple_authz_policy_file

Required

true

Suppress Parameter Validation: Excluded Wire Encryption Protocols

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Excluded Wire Encryption Protocols parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_ssl_exclude_protocols

Required

true

Suppress Parameter Validation: Knox SSO browser User-Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SSO browser User-Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_browser_useragent

Required

true

Suppress Parameter Validation: Knox SSO provider URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SSO provider URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_providerurl

Required

true

Suppress Parameter Validation: Knox SSO Public-Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SSO Public-Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_publickey

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/atlas-application.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Atlas Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Atlas Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ranger Atlas Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Atlas Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Atlas Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Atlas Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Atlas Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Atlas Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Atlas Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Atlas Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Atlas Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Atlas Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Atlas Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_atlas_server_unexpected_exits

Required

true

Suppress Health Test: Atlas Server Canary

Description

Whether to suppress the results of the Atlas Server Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_atlas_server_canary

Required

true

Gateway

Advanced

Atlas Client Advanced Configuration Snippet (Safety Valve) for atlas-conf/atlas-client.properties

Description

For advanced use only, a string to be inserted into the client configuration for atlas-conf/atlas-client.properties.

Related Name

Default Value

API Name

atlas-conf/atlas-client.properties_client_config_safety_valve

Required

false

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/atlas

API Name

client_config_root_dir

Required

true

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Security

Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

atlas.kafka.ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Gateway TLS/SSL Trust Store Password

Description

The password for the Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

atlas.kafka.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Parameter Validation: Atlas Client Advanced Configuration Snippet (Safety Valve) for atlas-conf/atlas-client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Client Advanced Configuration Snippet (Safety Valve) for atlas-conf/atlas-client.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas-conf/atlas-client.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Service-Wide

Advanced

Atlas Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ATLAS_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

atlas

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

atlas

API Name

process_username

Required

true

Monitoring

Healthy Atlas Server Monitoring Thresholds

Description

The health test thresholds of the overall Atlas Server health. The check returns "Concerning" health if the percentage of "Healthy" Atlas Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Atlas Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 90.0 %

API Name

ATLAS_ATLAS_SERVER_healthy_thresholds

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HBase Service

Description

Name of the HBase service that this Atlas service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

true

HDFS Service

Description

Name of the HDFS service that this Atlas service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

KAFKA Service

Description

Name of the KAFKA service that this Atlas service instance depends on

Related Name

Default Value

API Name

kafka_service

Required

true

Enable Kerberos Authentication

Description

Indicates whether Kerberos is enabled.

Related Name

atlas.authentication.method.kerberos

Default Value

false

API Name

kerberos.auth.enable

Required

false

Ranger Atlas Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_atlas_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/atlas

API Name

ranger_atlas_plugin_hdfs_audit_directory

Required

false

RANGER Service

Description

Name of the RANGER service that this Atlas service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Solr Service

Description

Name of the Solr service that this Atlas service instance depends on

Related Name

Default Value

API Name

solr_service

Required

true

Suppressions

Suppress Configuration Validator: Atlas Client Advanced Configuration Snippet (Safety Valve) for atlas-conf/atlas-client.properties

Description

Whether to suppress configuration warnings produced by the Atlas Client Advanced Configuration Snippet (Safety Valve) for atlas-conf/atlas-client.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas-conf/atlas-client.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Admin Password

Description

Whether to suppress configuration warnings produced by the Admin Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_admin_password

Required

true

Suppress Configuration Validator: Admin Username

Description

Whether to suppress configuration warnings produced by the Admin Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_admin_username

Required

true

Suppress Configuration Validator: Path to Credentials for File-based Login.

Description

Whether to suppress configuration warnings produced by the Path to Credentials for File-based Login. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_file_filename

Required

true

Suppress Configuration Validator: AD Base DN

Description

Whether to suppress configuration warnings produced by the AD Base DN configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_base_dn

Required

true

Suppress Configuration Validator: AD Bind DN Username

Description

Whether to suppress configuration warnings produced by the AD Bind DN Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_bind_dn

Required

true

Suppress Configuration Validator: AD Bind DN Password

Description

Whether to suppress configuration warnings produced by the AD Bind DN Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_bind_password

Required

true

Suppress Configuration Validator: AD User Default Role

Description

Whether to suppress configuration warnings produced by the AD User Default Role configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_default_role

Required

true

Suppress Configuration Validator: AD Domain Name (Only for AD)

Description

Whether to suppress configuration warnings produced by the AD Domain Name (Only for AD) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_domain

Required

true

Suppress Configuration Validator: AD URL

Description

Whether to suppress configuration warnings produced by the AD URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_url

Required

true

Suppress Configuration Validator: AD User Search Filter

Description

Whether to suppress configuration warnings produced by the AD User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_ad_user_searchfilter

Required

true

Suppress Configuration Validator: LDAP DN

Description

Whether to suppress configuration warnings produced by the LDAP DN configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_base_dn

Required

true

Suppress Configuration Validator: LDAP Bind DN Username

Description

Whether to suppress configuration warnings produced by the LDAP Bind DN Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_bind_dn

Required

true

Suppress Configuration Validator: LDAP Bind DN Password

Description

Whether to suppress configuration warnings produced by the LDAP Bind DN Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_bind_password

Required

true

Suppress Configuration Validator: LDAP User Default Role

Description

Whether to suppress configuration warnings produced by the LDAP User Default Role configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_default_role

Required

true

Suppress Configuration Validator: LDAP Group-Role Attribute

Description

Whether to suppress configuration warnings produced by the LDAP Group-Role Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_grouproleattribute

Required

true

Suppress Configuration Validator: LDAP Group-Search Base

Description

Whether to suppress configuration warnings produced by the LDAP Group-Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_groupsearchbase

Required

true

Suppress Configuration Validator: LDAP Group-Search Filter

Description

Whether to suppress configuration warnings produced by the LDAP Group-Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_groupsearchfilter

Required

true

Suppress Configuration Validator: LDAP Server URL

Description

Whether to suppress configuration warnings produced by the LDAP Server URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_url

Required

true

Suppress Configuration Validator: LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the LDAP User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_user_searchfilter

Required

true

Suppress Configuration Validator: User DN Pattern

Description

Whether to suppress configuration warnings produced by the User DN Pattern configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_authentication_method_ldap_userdnpattern

Required

true

Suppress Configuration Validator: Atlas Max Heapsize

Description

Whether to suppress configuration warnings produced by the Atlas Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_max_heap_size

Required

true

Suppress Configuration Validator: Knox Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_groups

Required

true

Suppress Configuration Validator: Knox Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_hosts

Required

true

Suppress Configuration Validator: Knox Proxy User Users

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyuser_knox_users

Required

true

Suppress Configuration Validator: Proxy Users

Description

Whether to suppress configuration warnings produced by the Proxy Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_proxyusers

Required

true

Suppress Configuration Validator: Server Bind Address

Description

Whether to suppress configuration warnings produced by the Server Bind Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_bind_address

Required

true

Suppress Configuration Validator: Server HTTP port

Description

Whether to suppress configuration warnings produced by the Server HTTP port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_http_port

Required

true

Suppress Configuration Validator: Server HTTPS Port

Description

Whether to suppress configuration warnings produced by the Server HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_https_port

Required

true

Suppress Configuration Validator: Atlas Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Atlas Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Simple Authz policy file

Description

Whether to suppress configuration warnings produced by the Simple Authz policy file configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_simple_authz_policy_file

Required

true

Suppress Configuration Validator: Excluded Wire Encryption Protocols

Description

Whether to suppress configuration warnings produced by the Excluded Wire Encryption Protocols configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_ssl_exclude_protocols

Required

true

Suppress Configuration Validator: Knox SSO browser User-Agent

Description

Whether to suppress configuration warnings produced by the Knox SSO browser User-Agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_browser_useragent

Required

true

Suppress Configuration Validator: Knox SSO provider URL

Description

Whether to suppress configuration warnings produced by the Knox SSO provider URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_providerurl

Required

true

Suppress Configuration Validator: Knox SSO Public-Key

Description

Whether to suppress configuration warnings produced by the Knox SSO Public-Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas_sso_knox_publickey

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/atlas-application.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-audit.xml

Description

Whether to suppress configuration warnings produced by the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-security.xml

Description

Whether to suppress configuration warnings produced by the Atlas Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-atlas-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-atlas-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Atlas Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Atlas Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Atlas Server Log Directory

Description

Whether to suppress configuration warnings produced by the Atlas Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ranger Atlas Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Atlas Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Atlas Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Atlas Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Atlas Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Atlas Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_atlas_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Atlas Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Atlas Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Atlas Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Atlas Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Atlas Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Atlas Server TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Atlas Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Atlas Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Atlas Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Atlas Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Atlas Server Count Validator

Description

Whether to suppress configuration warnings produced by the Atlas Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_server_count_validator

Required

true

Suppress Parameter Validation: Atlas Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_service_env_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Atlas Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Atlas Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_atlas_plugin_hdfs_audit_directory

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Atlas Server Health

Description

Whether to suppress the results of the Atlas Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_atlas_atlas_server_healthy

Required

true

Core Configuration Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hadoop

API Name

client_config_root_dir

Required

true

Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hadoop-env.sh

Related Name

Default Value

API Name

core_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

core_client_java_opts

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

core_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Service-Wide

Advanced

Core Configuration Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

CORE_SETTINGS_service_env_safety_valve

Required

false

Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to all roles and client configurations in this HDFS service as well as all its dependent services. Any configs added here will be overridden by their default values in HDFS (which can be found in hdfs-default.xml).

Related Name

Default Value

API Name

core_site_safety_valve

Required

false

HDFS Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

For advanced use only, a string to be inserted into ssl-client.xml. Applies cluster-wide, but can be overridden by individual services.

Related Name

Default Value

API Name

hdfs_ssl_client_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as (except the HttpFS server, which has its own group)

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.

- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Default Filesystem

Description

The defaultFs to use in the cluster. Leave this blank if the cluster has a storage service which should be used as the defaultFs.

Related Name

core.defaultFs

Default Value

API Name

core_defaultfs

Required

false

Object Store Service

Description

Select an Object Store service to enable cloud storage support. Once enabled, the cloud storage can be used in Impala and Hue services, via fully-qualified URIs.

Related Name

Default Value

API Name

object_store_service

Required

false

Set Rules to Map Kerberos Principals to Lower Case Short Names

Description

Adds mapping rules to map Kerberos principals to lower case short names that will be inserted before the default rule. After changing this value and restarting the service, any services depending on this one must be restarted as well.

Related Name

Default Value

false

API Name

set_auth_to_local_to_lowercase

Required

false

Proxy

HDFS Proxy User Groups

Description

Comma-delimited list of groups to allow the HDFS user to impersonate. The default '*' allows all groups. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.hdfs.groups

Default Value

*

API Name

hdfs_proxy_user_groups_list

Required

false

HDFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HDFS user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.hdfs.hosts

Default Value

*

API Name

hdfs_proxy_user_hosts_list

Required

false

Hive Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Hive user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.hive.groups

Default Value

*

API Name

hive_proxy_user_groups_list

Required

false

Hive Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Hive user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.hive.hosts

Default Value

*

API Name

hive_proxy_user_hosts_list

Required

false

HTTP Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the HTTP user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'. This is used by WebHCat.

Related Name

hadoop.proxyuser.HTTP.groups

Default Value

*

API Name

HTTP_proxy_user_groups_list

Required

false

HTTP Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HTTP user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'. This is used by WebHCat.

Related Name

hadoop.proxyuser.HTTP.hosts

Default Value

*

API Name

HTTP_proxy_user_hosts_list

Required

false

HttpFS Proxy User Groups

Description

Comma-delimited list of groups to allow the HttpFS user to impersonate. The default '*' allows all groups. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.httpfs.groups

Default Value

*

API Name

httpfs_proxy_user_groups_list

Required

false

HttpFS Proxy User Hosts

Description

Comma-delimited list of hosts where you allow the HttpFS user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.httpfs.hosts

Default Value

*

API Name

httpfs_proxy_user_hosts_list

Required

false

Hue Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Hue user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.hue.groups

Default Value

*

API Name

hue_proxy_user_groups_list

Required

false

Hue Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Hue user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.hue.hosts

Default Value

*

API Name

hue_proxy_user_hosts_list

Required

false

Impala Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Impala user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.impala.groups

Default Value

*

API Name

impala_proxy_user_groups_list

Required

false

Impala Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Impala user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.impala.hosts

Default Value

*

API Name

impala_proxy_user_hosts_list

Required

false

Knox Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Knox user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.knox.groups

Default Value

*

API Name

knox_proxy_user_groups_list

Required

false

Knox Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Knox user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.knox.hosts

Default Value

*

API Name

knox_proxy_user_hosts_list

Required

false

Kudu Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Kudu user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.kudu.groups

Default Value

*

API Name

kudu_proxy_user_groups_list

Required

false

Kudu Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Kudu user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.kudu.hosts

Default Value

*

API Name

kudu_proxy_user_hosts_list

Required

false

Livy Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Livy user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.livy.groups

Default Value

*

API Name

livy_proxy_user_groups_list

Required

false

Livy Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Livy user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.livy.hosts

Default Value

*

API Name

livy_proxy_user_hosts_list

Required

false

Oozie Proxy User Groups

Description

Allows the oozie superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.oozie.groups

Default Value

*

API Name

oozie_proxy_user_groups_list

Required

false

Oozie Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the oozie user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.oozie.hosts

Default Value

*

API Name

oozie_proxy_user_hosts_list

Required

false

Phoenix Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Phoenix user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.phoenix.groups

Default Value

*

API Name

phoenix_proxy_user_groups_list

Required

false

Phoenix Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Phoenix user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.phoenix.hosts

Default Value

*

API Name

phoenix_proxy_user_hosts_list

Required

false

Service Monitor Proxy User Groups

Description

Allows the Cloudera Service Monitor user to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. This property is used only if Service Monitor is using a different Kerberos principal than the Hue service. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.smon.groups

Default Value

*

API Name

smon_proxy_user_groups_list

Required

false

Service Monitor Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Cloudera Service Monitor user to impersonate other users. The default '*' allows all hosts. This property is used only if Service Monitor is using a different Kerberos principal than the Hue service. To disable entirely, use a string that does not correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.smon.hosts

Default Value

*

API Name

smon_proxy_user_hosts_list

Required

false

Telemetry Publisher Proxy User Groups

Description

Allows the Cloudera Telemetry Publisher user to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. This property is used only if Telemetry Publisher is

using a different Kerberos principal than the Hue service. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.telepub.groups

Default Value

*

API Name

telepub_proxy_user_groups_list

Required

false

Telemetry Publisher Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Cloudera Telemetry Publisher user to impersonate other users. The default '*' allows all hosts. This property is used only if Telemetry Publisher is using a different Kerberos principal than the Hue service. To disable entirely, use a string that does not correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.telepub.hosts

Default Value

*

API Name

telepub_proxy_user_hosts_list

Required

false

YARN Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the YARN user to impersonate. The default '*' allows all groups. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.yarn.groups

Default Value

*

API Name

yarn_proxy_user_groups_list

Required

false

YARN Proxy User Hosts

Description

Comma-delimited list of hosts that you want to allow the YARN user to impersonate. The default '*' allows all hosts. To disable entirely, use a string that does not correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.yarn.hosts

Default Value

*

API Name

yarn_proxy_user_hosts_list

Required

false

Security

Additional Rules to Map Kerberos Principals to Short Names

Description

Additional mapping rules that will be inserted before rules generated from the list of trusted realms and before the default rule. After changing this value and restarting the service, any services depending on this one must be restarted as well. The hadoop.security.auth_to_local property is configured using this information. Default rules are generated by Cloudera Manager and substituted in place of the literal {DEFAULT_RULES} if it is specified in this value.

Related Name

Default Value

DEFAULT_RULES

API Name

extra_auth_to_local_rules

Required

false

Authorized Admin Groups

Description

Comma-separated list of groups authorized to perform admin operations on Hadoop. This is emitted only if authorization is enabled.

Related Name

Default Value

API Name

hadoop_authorized_admin_groups

Required

false

Authorized Admin Users

Description

Comma-separated list of users authorized to perform admin operations on Hadoop. This is emitted only if authorization is enabled.

Related Name

Default Value

*

API Name

hadoop_authorized_admin_users

Required

false

Authorized Groups

Description

Comma-separated list of groups authorized to used Hadoop. This is emitted only if authorization is enabled.

Related Name

Default Value

API Name

hadoop_authorized_groups

Required

false

Authorized Users

Description

Comma-separated list of users authorized to used Hadoop. This is emitted only if authorization is enabled.

Related Name

Default Value

*

API Name

hadoop_authorized_users

Required

false

Hadoop User Group Mapping Search Base

Description

The search base for the LDAP connection. This is a distinguished name, and will typically be the root of the LDAP directory.

Related Name

hadoop.security.group.mapping.ldap.base

Default Value

API Name

hadoop_group_mapping_ldap_base

Required

false

Hadoop User Group Mapping LDAP Bind User Password

Description

The password of the bind user.

Related Name

hadoop.security.group.mapping.ldap.bind.password

Default Value

API Name

hadoop_group_mapping_ldap_bind_passwd

Required

false

Hadoop User Group Mapping LDAP Bind User Distinguished Name

Description

Distinguished name of the user to bind to AD as for user authentication search/bind and group lookup for role authorization. For openLDAP based directories this should be a DN string, for Active Directory this can be just a username, combined with the "Active Directory Domain" value for login. For example username in the field and example.com in the active directory domain will result in the User Principal Name value of username@example.com being used to bind. If you put a UPM value here, do not over-configure the "active directory domain" field otherwise you will end up presenting username@example.com@example.com for binds. AD will accept a UPN value or the DN value as a valid Bind DN; An example of a Distinguished Name (DN): CN=cdh admin,OU=svcaccount,DC=example,DC=com An example of a UPN value: cdhadmin@example.com

Related Name

hadoop.security.group.mapping.ldap.bind.user

Default Value

API Name

hadoop_group_mapping_ldap_bind_user

Required

false

Hadoop User Group Mapping LDAP Group Search Filter

Description

An additional filter to use when searching for groups.

Related Name

hadoop.security.group.mapping.ldap.search.filter.group

Default Value

(objectClass=group)

API Name

hadoop_group_mapping_ldap_group_filter

Required

false

Hadoop User Group Mapping LDAP Group Name Attribute

Description

The attribute of the group object that identifies the group name. The default will usually be appropriate for all LDAP systems.

Related Name

hadoop.security.group.mapping.ldap.search.attr.group.name

Default Value

cn

API Name

hadoop_group_mapping_ldap_group_name_attr

Required

false

Hadoop User Group Mapping LDAP TLS/SSL Truststore

Description

File path to a jks-format truststore containing the TLS/SSL certificate used sign the LDAP server's certificate. Note that in previous releases this was erroneously referred to as a "keystore".

Related Name

hadoop.security.group.mapping.ldap.ssl.keystore

Default Value

API Name

hadoop_group_mapping_ldap_keystore

Required

false

Hadoop User Group Mapping LDAP TLS/SSL Truststore Password

Description

The password for the TLS/SSL truststore.

Related Name

hadoop.security.group.mapping.ldap.ssl.keystore.password

Default Value

API Name

hadoop_group_mapping_ldap_keystore_passwd

Required

false

Hadoop User Group Mapping LDAP Group Membership Attribute

Description

The attribute of the group object that identifies the users that are members of the group. The default will usually be appropriate for any LDAP installation.

Related Name

hadoop.security.group.mapping.ldap.search.attr.member

Default Value

member

API Name

hadoop_group_mapping_ldap_member_attr

Required

false

Hadoop User Group Mapping LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind

to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

hadoop.security.group.mapping.ldap.url

Default Value

API Name

hadoop_group_mapping_ldap_url

Required

false

Hadoop User Group Mapping LDAP TLS/SSL Enabled

Description

Whether or not to use TLS/SSL when connecting to the LDAP server.

Related Name

hadoop.security.group.mapping.ldap.use.ssl

Default Value

false

API Name

hadoop_group_mapping_ldap_use_ssl

Required

false

Hadoop User Group Mapping LDAP User Search Filter

Description

An additional filter to use when searching for LDAP users. The default will usually be appropriate for Active Directory installations. If connecting to a generic LDAP server, "sAMAccountName" will likely be replaced with "uid". {0} is a special string used to denote where the username fits into the filter.

Related Name

hadoop.security.group.mapping.ldap.search.filter.user

Default Value

(&(objectClass=user)(sAMAccountName=0))

API Name

hadoop_group_mapping_ldap_user_filter

Required

false

Hadoop HTTP Authentication Cookie Domain

Description

The domain to use for the HTTP cookie that stores the authentication token. In order for authentiation to work correctly across all Hadoop nodes' web-consoles the domain must be correctly set. Important: when using IP addresses, browsers ignore cookies with domain settings. For this setting to work properly all nodes in the cluster must be configured to generate URLs with hostname.domain names on it.

Related Name

Default Value

API Name

hadoop_http_auth_cookie_domain

Required

false

Hadoop RPC Protection

Description

Quality of protection for secured RPC connections between NameNode and HDFS clients. For effective RPC protection, enable Kerberos authentication.

Related Name

hadoop.rpc.protection

Default Value

authentication

API Name

hadoop_rpc_protection

Required

false

Hadoop Secure Authentication

Description

Choose the authentication mechanism used by Hadoop

Related Name

hadoop.security.authentication

Default Value

simple

API Name

hadoop_security_authentication

Required

false

Hadoop Secure Authorization

Description

Enable authorization

Related Name

hadoop.security.authorization

Default Value

false

API Name

hadoop_security_authorization

Required

false

Hadoop User Group Mapping Implementation

Description

Class for user to group mapping (get groups for a given user).

Related Name

hadoop.security.group.mapping

Default Value

org.apache.hadoop.security.ShellBasedUnixGroupsMapping

API Name

hadoop_security_group_mapping

Required

false

Encryption Key Default Length

Description

The length (bits) of keys we want the KeyProvider to produce. Key length defines the upper-bound on an algorithm's security, ideally, it would coincide with the lower-bound on an algorithm's security.

Related Name

hadoop.security.key.default.bitlength

Default Value

128

API Name

hdfs_encryption_key_length

Required

false

Hadoop TLS/SSL Enabled

Description

Enable TLS/SSL encryption for HDFS, MapReduce, and YARN web UIs, as well as encrypted shuffle for MapReduce and YARN.

Related Name

hadoop.ssl.enabled

Default Value

false

API Name

hdfs_hadoop_ssl_enabled

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hdfs

API Name

kerberos_princ_name

Required

true

Log and Query Redaction Policy

Description

Note: Do not edit this property in the classic layout. Switch to the new layout to use preconfigured redaction rules and test your rules inline.Use this property to define a list of rules to be followed for redacting sensitive information from log files and query strings. Click + to add a new redaction rule. You can choose one of the preconfigured rules or add a custom rule. When specifying a custom rule, the Search field should contain a regular expression that will be matched against the data. If a match is found, it is replaced by the contents of the Replace field.Trigger is an optional field. It can be used to specify a simple string to be searched in the data. If the string is found, the redactor attempts to find a match for the Search regex. If no trigger is specified, redaction occurs by matching the Search regular expression. Use the Trigger field to enhance performance: simple string matching is faster than regular expression matching.Test your rules by entering sample text into the Test Redaction Rules text box and clicking Test Redaction. If no rules match, the text you entered is returned unchanged.

Related Name

redaction_policy

Default Value

version: 1, rules: [description: Redact passwords from json files, trigger: password, search: \password\[ ]*:[ ]*\[^\]+\, caseSensitive: false, replace: \password\: \LOG-REDACTED\ , description: Redact password\u003d and password:, trigger: password, search: password[:\u003d][^ \\\\\]+, caseSensitive: false, replace: password\u003dLOG-REDACTED , description: Redact passwd\u003d and passwd:, trigger: passwd, search: passwd[:\u003d][^ \\\\\]+, caseSensitive: false, replace: passwd\u003dLOG-REDACTED , description: Redact pass\u003d and pass:, trigger: pass, search: pass[:\u003d][^ \\\\\]+, caseSensitive: false, replace: pass\u003dLOG-REDACTED , description: Redact PASSWORD, , trigger: PASSWORD, , search: PASSWORD, [^\\\\\]+, caseSensitive: false, replace: PASSWORD, LOG-REDACTED , description: Redact secret\u003d and secret:, trigger: secret, search: secret[:\u003d][^ \\\\\]+, caseSensitive: false, replace: secret \u003dLOG-REDACTED , description: Credit Card numbers (with separator), search: \\b\\d4[^ \\w:]\\d4[^\\w:]\\d4[^\\w:]\\d4\\b, caseSensitive: true, replace: XXXX-XXXX-XXXX-XXXX , description: Social Security numbers (with separator), search: \\b\\d3[^\\w:]\\d2[^\\w:]\\d4\\b, caseSensitive: true, replace: XXX-XX-XXXX]

API Name

redaction_policy

Required

false

Enable Log and Query Redaction

Description

Enable/Disable the Log and Query Redaction Policy for this cluster.

Related Name

redaction_policy_enabled

Default Value

true

API Name

redaction_policy_enabled

Required

false

Enable Security Audit Logger

Description

Enable security audit logger for HDFS and dependent services

Related Name

security_logger_enabled

Default Value

true

API Name

security_logger_enabled

Required

false

Cluster-Wide Default TLS/SSL Client Truststore Location

Description

Path to the TLS/SSL client truststore file. Defines a cluster-wide default that can be overridden by individual services. This truststore must be in JKS format. The truststore contains certificates of trusted servers, or of Certificate Authorities trusted to identify servers. The contents of the truststore can be modified without restarting any roles. By default, changes to its contents are picked up within ten seconds. If not set, the default Java truststore is used to verify certificates.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Cluster-Wide Default TLS/SSL Client Truststore Password

Description

Password for the TLS/SSL client truststore. Defines a cluster-wide default that can be overridden by individual services.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

HTTP Strict Transport Security

Description

HTTP Strict Transport Security (HSTS) ensures that a web browser does not load the service information using http protocol.

Related Name

hadoop.http.header.Strict_Transport_Security

Default Value

max-age=0; includeSubDomains

API Name

strict_transport_security

Required

false

Trusted Kerberos Realms

Description

List of Kerberos realms that Hadoop services should trust. If empty, defaults to the default_realm property configured in the krb5.conf file. After changing this value and restarting the service, all services depending on this service must also be restarted. Adds mapping rules for each domain to the hadoop.security.auth_to_local property in core-site.xml.

Related Name

Default Value

API Name

trusted_realms

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_java_opts

Required

true

Suppress Configuration Validator: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Default Filesystem

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Filesystem parameter.

Related Name

Default Value

false

API Name

service_config_suppression_core_defaultfs

Required

true

Suppress Parameter Validation: Core Configuration Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Core Configuration Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_core_settings_service_env_safety_valve

Required

true

Suppress Parameter Validation: Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_core_site_safety_valve

Required

true

Suppress Parameter Validation: Additional Rules to Map Kerberos Principals to Short Names

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Rules to Map Kerberos Principals to Short Names parameter.

Related Name

Default Value

false

API Name

service_config_suppression_extra_auth_to_local_rules

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Authorized Admin Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Authorized Admin Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_authorized_admin_groups

Required

true

Suppress Parameter Validation: Authorized Admin Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Authorized Admin Users parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_authorized_admin_users

Required

true

Suppress Parameter Validation: Authorized Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Authorized Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_authorized_groups

Required

true

Suppress Parameter Validation: Authorized Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Authorized Users parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_authorized_users

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping Search Base parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_base

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP Bind User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP Bind User Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_bind_passwd

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP Bind User Distinguished Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP Bind User Distinguished Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_bind_user

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP Group Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP Group Search Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_group_filter

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP Group Name Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP Group Name Attribute parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_group_name_attr

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP TLS/SSL Truststore

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP TLS/SSL Truststore parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_keystore

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP TLS/SSL Truststore Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP TLS/SSL Truststore Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_keystore_passwd

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP Group Membership Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP Group Membership Attribute parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_member_attr

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_url

Required

true

Suppress Parameter Validation: Hadoop User Group Mapping LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop User Group Mapping LDAP User Search Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_group_mapping_ldap_user_filter

Required

true

Suppress Parameter Validation: Hadoop HTTP Authentication Cookie Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop HTTP Authentication Cookie Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_http_auth_cookie_domain

Required

true

Suppress Configuration Validator: HDFS Authentication And Authorization Validation

Description

Whether to suppress configuration warnings produced by the HDFS Authentication And Authorization Validation configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_authentication_and_authorization_validator

Required

true

Suppress Parameter Validation: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_proxy_user_groups_list

Required

true

Suppress Parameter Validation: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: HDFS Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Advanced Configuration Snippet (Safety Valve) for ssl-client.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_ssl_client_safety_valve

Required

true

Suppress Parameter Validation: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_http_proxy_user_groups_list

Required

true

Suppress Parameter Validation: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_http_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_httpfs_proxy_user_groups_list

Required

true

Suppress Parameter Validation: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_httpfs_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Impala Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Impala Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Knox Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Knox Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Kudu Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kudu_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Kudu Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kudu_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_livy_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_livy_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Phoenix Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Phoenix Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_phoenix_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Phoenix Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Phoenix Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_phoenix_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Log and Query Redaction Policy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Log and Query Redaction Policy parameter.

Related Name

Default Value

false

API Name

service_config_suppression_redaction_policy

Required

true

Suppress Configuration Validator: Redaction Policy Validator

Description

Whether to suppress configuration warnings produced by the Redaction Policy Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_redaction_policy_validator

Required

true

Suppress Configuration Validator: Hadoop RPC Protection validator

Description

Whether to suppress configuration warnings produced by the Hadoop RPC Protection validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_rpc_protection_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Service Monitor Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Service Monitor Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Cluster-Wide Default TLS/SSL Client Truststore Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cluster-Wide Default TLS/SSL Client Truststore Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Cluster-Wide Default TLS/SSL Client Truststore Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cluster-Wide Default TLS/SSL Client Truststore Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: HTTP Strict Transport Security

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Strict Transport Security parameter.

Related Name

Default Value

false

API Name

service_config_suppression_strict_transport_security

Required

true

Suppress Parameter Validation: Telemetry Publisher Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_telepub_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Telemetry Publisher Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_telepub_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Trusted Kerberos Realms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Trusted Kerberos Realms parameter.

Related Name

Default Value

false

API Name

service_config_suppression_trusted_realms

Required

true

Suppress Parameter Validation: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_proxy_user_groups_list

Required

true

Suppress Parameter Validation: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_proxy_user_hosts_list

Required

true

Cruise Control Properties in Cloudera Runtime 7.2.18

Role groups:

Cruise Control Server

Advanced

Cruise Control Server Advanced Configuration Snippet (Safety Valve) for auth.credentials

Description

For advanced use only. A string to be inserted into auth.credentials for this role only.

Related Name

Default Value

API Name

auth.credentials_role_safety_valve

Required

false

Cruise Control Server Advanced Configuration Snippet (Safety Valve) for capacity.json

Description

For advanced use only. A string to be inserted into capacity.json for this role only.

Related Name

Default Value

API Name

capacity.json_role_safety_valve

Required

false

Cruise Control Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

CRUISE_CONTROL_SERVER_role_env_safety_valve

Required

false

Cruise Control Server Advanced Configuration Snippet (Safety Valve) for cruisecontrol.properties

Description

For advanced use only. A string to be inserted into cruisecontrol.properties for this role only.

Related Name

Default Value

API Name

cruisecontrol.properties_role_safety_valve

Required

false

Cruise Control Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

For advanced use only. A string to be inserted into ssl.properties for this role only.

Related Name

Default Value

API Name

ssl.properties_role_safety_valve

Required

false

Logs

Cruise Control Server Log Directory

Description

The log directory for log files of the role Cruise Control Server.

Related Name

log_dir

Default Value

/var/log/cruisecontrol

API Name

log_dir

Required

false

Cruise Control Server Logging Threshold

Description

The minimum log level for Cruise Control Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Cruise Control Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Cruise Control Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Cruise Control Server Max Log Size

Description

The maximum size, in megabytes, per log file for Cruise Control Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

cruise_control_server_fd_thresholds

Required

false

Cruise Control Server Host Health Test

Description

When computing the overall Cruise Control Server health, consider the host's health.

Related Name

Default Value

true

API Name

cruise_control_server_host_health_enabled

Required

false

Cruise Control Server Process Health Test

Description

Enables the health test that the Cruise Control Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

cruise_control_server_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters,

$ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Anomaly Detection Goals

Description

The list of goals that the anomaly detector should detect if they are violated. It must be a subset of Self-Healing Goals and thus also of Default Goals.

Related Name

anomaly.detection.goals

Default Value

com.linkedin.kafka.cruisecontrol.analyzer.goals.RackAwareGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskCapacityGoal

API Name

anomaly.detection.goals

Required

true

Anomaly Notifier Class

Description

The notifier class to trigger an alert when an anomaly is violated.

Related Name

anomaly.notifier.class

Default Value

com.linkedin.kafka.cruisecontrol.detector.notifier.NoopNotifier

API Name

anomaly.notifier.class

Required

false

ADMIN Level Users

Description

The list of ADMIN level users.

Related Name

auth_admins

Default Value

API Name

auth_admins

Required

false

Authentication Method

Description

Authentication method that Cruise Control uses to authenticate clients.

Related Name

auth_method

Default Value

none

API Name

auth_method

Required

false

USER Level Users

Description

The list of USER level users.

Related Name

auth_users

Default Value

API Name

auth_users

Required

false

VIEWER Level Users

Description

The list of VIEWER level users.

Related Name

auth_viewers

Default Value

API Name

auth_viewers

Required

false

Broker Metrics Topic

Description

The config for the Kafka sample store to save the model training samples.

Related Name

broker.metric.sample.store.topic

Default Value

__KafkaCruiseControlModelTrainingSamples

API Name

broker.metric.sample.store.topic

Required

true

Broker Metrics Window Size

Description

The broker metrics window size in milliseconds.

Related Name

broker.metrics.window.ms

Default Value

5 minute(s)

API Name

broker.metrics.window.ms

Required

true

Default CPU Capacity

Description

Default CPU capacity in capacity.json config.

Related Name

capacity.default.cpu

Default Value

100 %

API Name

capacity.default.cpu

Required

true

Default Incoming Network Capacity

Description

Default incoming network capacity in capacity.json config.

Related Name

capacity.default.network-in

Default Value

100000 KiB

API Name

capacity.default.network-in

Required

true

Default Outgoing Network Capacity

Description

Default outgoing network capacity in capacity.json config.

Related Name

capacity.default.network-out

Default Value

100000 KiB

API Name

capacity.default.network-out

Required

true

CPU Balance Threshold

Description

The maximum allowed extent of unbalance for CPU utilization, enforced by the goal optimization. For example, 1.10 means the highest CPU usage of a broker should not be above 1.10x of average CPU utilization of all the brokers.

Related Name

cpu.balance.threshold

Default Value

1.1

API Name

cpu.balance.threshold

Required

false

CPU Capacity Threshold

Description

The maximum percentage of the total broker.cpu.capacity that is allowed to be used on a broker, enforced by the goal optimization. The analyzer will enforce a hard goal that the CPU utilization of a broker cannot be higher than (broker.cpu.capacity * cpu.capacity.threshold).

Related Name

cpu.capacity.threshold

Default Value

0.7

API Name

cpu.capacity.threshold

Required

false

Default Goals

Description

The list of goals to pre-compute proposals or to compute completeness requirements if Self-Healing Goals is not specified.

Related Name

default.goals

Default Value

com.linkedin.kafka.cruisecontrol.analyzer.goals.RackAwareGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkInboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkOutboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.CpuCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.PotentialNwOutGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkInboundUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkOutboundUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.CpuUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.TopicReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.LeaderReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.LeaderBytesInDistributionGoal

API Name

default.goals

Required

true

Disk Balance Threshold

Description

The maximum allowed extent of unbalance for disk utilization, enforced by the goal optimization. For example, 1.10 means the highest disk usage of a broker should not be above 1.10x of average disk utilization of all the brokers.

Related Name

disk.balance.threshold

Default Value

1.1

API Name

disk.balance.threshold

Required

false

Disk Capacity Threshold

Description

The maximum percentage of the total broker.disk.capacity that is allowed to be used on a broker, enforced by the goal optimization. The analyzer will enforce a hard goal that the disk usage of a broker cannot be higher than (broker.disk.capacity * disk.capacity.threshold).

Related Name

disk.capacity.threshold

Default Value

0.8

API Name

disk.capacity.threshold

Required

false

Supported Goals

Description

The list of supported goals.

Related Name

goals

Default Value

com.linkedin.kafka.cruisecontrol.analyzer.goals.RackAwareGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkInboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkOutboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.CpuCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.PotentialNwOutGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkInboundUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkOutboundUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.CpuUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.TopicReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.LeaderReplicaDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.LeaderBytesInDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.PreferredLeaderElectionGoal
com.linkedin.kafka.cruisecontrol.analyzer.kafkaassigner.KafkaAssignerDiskUsageDistributionGoal
com.linkedin.kafka.cruisecontrol.analyzer.kafkaassigner.KafkaAssignerEvenRackAwareGoal

API Name

goals

Required

true

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

1 minute(s)

API Name

graceful_stop_timeout

Required

false

Hard Goals

Description

The list of goals that any optimization proposal must fulfill if Cruise Control runs in non-kafka-assigner mode and skip_hard_goal_check parameter is not set in the request.

Related Name

hard.goals

Default Value

com.linkedin.kafka.cruisecontrol.analyzer.goals.RackAwareGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.ReplicaCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.DiskCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkInboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.NetworkOutboundCapacityGoal
com.linkedin.kafka.cruisecontrol.analyzer.goals.CpuCapacityGoal

API Name

hard.goals

Required

false

Leader Replica Count Balance Threshold

Description

The maximum allowed extent of unbalance for leader replica distribution, enforced by the goal optimization. For example, 1.10 means the highest leader replica count of a broker should not be above 1.10x of average leader replica count of all alive brokers.

Related Name

leader.replica.count.balance.threshold

Default Value

1.1

API Name

leader.replica.count.balance.threshold

Required

false

Metric Anomaly Finder Class

Description

A list of metric anomaly finder classes to identify metric anomalies.

Related Name

metric.anomaly.finder.class

Default Value

com.linkedin.kafka.cruisecontrol.detector.NoopMetricAnomalyFinder

API Name

metric.anomaly.finder.class

Required

false

Network Inbound Balance Threshold

Description

The maximum allowed extent of unbalance for network inbound usage, enforced by the goal optimization. For example, 1.10 means the highest network inbound usage of a broker should not be above 1.10x of average network inbound usage of all the brokers.

Related Name

network.inbound.balance.threshold

Default Value

1.1

API Name

network.inbound.balance.threshold

Required

false

Network Inbound Capacity Threshold

Description

The maximum percentage of the total broker.network.inbound.capacity that is allowed to be used on a broker, enforced by the goal optimization. The analyzer will enforce a hard goal that the disk usage of a broker cannot be higher than (broker.network.inbound.capacity * network.inbound.capacity.threshold).

Related Name

network.inbound.capacity.threshold

Default Value

0.8

API Name

network.inbound.capacity.threshold

Required

false

Network Outbound Balance Threshold

Description

The maximum allowed extent of unbalance for network outbound usage, enforced by the goal optimization. For example, 1.10 means the highest network outbound usage of a broker should not be above 1.10x of average network outbound usage of all the brokers.

Related Name

network.outbound.balance.threshold

Default Value

1.1

API Name

network.outbound.balance.threshold

Required

false

Network Outbound Capacity Threshold

Description

The maximum percentage of the total broker.network.outbound.capacity that is allowed to be used on a broker, enforced by the goal optimization. The analyzer will enforce a hard goal that the disk usage of a broker cannot be higher than (broker.network.outbound.capacity * network.outbound.capacity.threshold).

Related Name

network.outbound.capacity.threshold

Default Value

0.8

API Name

network.outbound.capacity.threshold

Required

false

Number of Broker Metric Windows

Description

The total number of windows to keep for broker metric samples.

Related Name

num.broker.metrics.windows

Default Value

5

API Name

num.broker.metrics.windows

Required

true

Number of Metric Fetchers

Description

The number of metric fetcher threads.

Related Name

num.metric.fetchers

Default Value

1

API Name

num.metric.fetchers

Required

true

Number of Partition Metric Windows

Description

The total number of windows to keep for partition metric samples.

Related Name

num.partition.metrics.windows

Default Value

5

API Name

num.partition.metrics.windows

Required

true

Partition Metrics Topic

Description

The config for the Kafka sample store to save the partition metric samples.

Related Name

partition.metric.sample.store.topic

Default Value

__KafkaCruiseControlPartitionMetricSamples

API Name

partition.metric.sample.store.topic

Required

true

Partition Metrics Window Size

Description

The partition metrics window size in milliseconds.

Related Name

partition.metrics.window.ms

Default Value

5 minute(s)

API Name

partition.metrics.window.ms

Required

true

Replica Count Balance Threshold

Description

The maximum allowed extent of unbalance for replica distribution, enforced by the goal optimization. For example, 1.10 means the highest replica count of a broker should not be above 1.10x of average replica count of all brokers.

Related Name

replica.count.balance.threshold

Default Value

1.1

API Name

replica.count.balance.threshold

Required

false

Self Healing Enabled

Description

Whether to enable self healing for all anomaly detectors, unless the particular anomaly detector is explicitly disabled.

Related Name

self.healing.enabled

Default Value

false

API Name

self.healing.enabled

Required

false

Self-Healing Goals

Description

The list of goals to be used for self-healing relevant anomalies. If empty, uses Default Goals for self-healing.

Related Name

self.healing.goals

Default Value

API Name

self.healing.goals

Required

false

Enable Trusted Proxy Fallback to Spnego

Description

If no doAs user is provided in Trusted Proxy authentication then it proceeds with using the service user for executing the request.

Related Name

trusted.proxy.spnego.fallback.enabled

Default Value

false

API Name

trusted.proxy.spnego.fallback.enabled

Required

false

Trusted Proxy Authentication Service

Description

The username part of the trusted proxy authentication service's principal.

Related Name

trusted_auth_service_user

Default Value

knox

API Name

trusted_auth_service_user

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Cruise Control Webserver Port

Description

The endpoint of the REST interface.

Related Name

webserver.http.port

Default Value

8899

API Name

webserver.http.port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Cruise Control Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Cruise Control Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Cruise Control Server TLS/SSL Trust Store Password

Description

The password for the Cruise Control Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Cruise Control Server

Description

Encrypt communication between clients and Cruise Control Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

webserver.ssl.enable

Default Value

false

API Name

ssl_enabled

Required

false

Cruise Control Server TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Cruise Control Server is acting as a TLS/SSL server.

Related Name

webserver.ssl.key.password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Cruise Control Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Cruise Control Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

webserver.ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Cruise Control Server TLS/SSL Server Keystore File Password

Description

The password for the Cruise Control Server keystore file.

Related Name

webserver.ssl.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Anomaly Detection Goals

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Anomaly Detection Goals parameter.

Related Name

Default Value

false

API Name

role_config_suppression_anomaly.detection.goals

Required

true

Suppress Parameter Validation: Anomaly Notifier Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Anomaly Notifier Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_anomaly.notifier.class

Required

true

Suppress Parameter Validation: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for auth.credentials

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for auth.credentials parameter.

Related Name

Default Value

false

API Name

role_config_suppression_auth.credentials_role_safety_valve

Required

true

Suppress Parameter Validation: ADMIN Level Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ADMIN Level Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_auth_admins

Required

true

Suppress Parameter Validation: USER Level Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the USER Level Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_auth_users

Required

true

Suppress Parameter Validation: VIEWER Level Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the VIEWER Level Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_auth_viewers

Required

true

Suppress Parameter Validation: Broker Metrics Topic

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Broker Metrics Topic parameter.

Related Name

Default Value

false

API Name

role_config_suppression_broker.metric.sample.store.topic

Required

true

Suppress Parameter Validation: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for capacity.json

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for capacity.json parameter.

Related Name

Default Value

false

API Name

role_config_suppression_capacity.json_role_safety_valve

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Cruise Control Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cruise_control_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for cruisecontrol.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for cruisecontrol.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cruisecontrol.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Default Goals

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Goals parameter.

Related Name

Default Value

false

API Name

role_config_suppression_default.goals

Required

true

Suppress Parameter Validation: Supported Goals

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Supported Goals parameter.

Related Name

Default Value

false

API Name

role_config_suppression_goals

Required

true

Suppress Parameter Validation: Hard Goals

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hard Goals parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hard.goals

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Cruise Control Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Cruise Control Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Metric Anomaly Finder Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metric Anomaly Finder Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metric.anomaly.finder.class

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Partition Metrics Topic

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Partition Metrics Topic parameter.

Related Name

Default Value

false

API Name

role_config_suppression_partition.metric.sample.store.topic

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Self-Healing Goals

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Self-Healing Goals parameter.

Related Name

Default Value

false

API Name

role_config_suppression_self.healing.goals

Required

true

Suppress Parameter Validation: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Cruise Control Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Cruise Control Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Cruise Control Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Cruise Control Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Cruise Control Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Trusted Proxy Authentication Service

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Trusted Proxy Authentication Service parameter.

Related Name

Default Value

false

API Name

role_config_suppression_trusted_auth_service_user

Required

true

Suppress Parameter Validation: Cruise Control Webserver Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Webserver Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver.http.port

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_cruise_control_cruise_control_server_unexpected_exits

Required

true

Service-Wide

Advanced

Cruise Control Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

CRUISE_CONTROL_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hadoop

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

cruisecontrol

API Name

process_username

Required

true

Monitoring

Cruise Control Server Role Health Test

Description

When computing the overall CRUISE_CONTROL health, consider Cruise Control Server's health

Related Name

Default Value

true

API Name

CRUISE_CONTROL_CRUISE_CONTROL_SERVER_health_enabled

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

KAFKA Service

Description

Name of the KAFKA service that this Cruise Control service instance depends on

Related Name

Default Value

API Name

kafka_service

Required

true

ZooKeeper Service

Description

Name of the ZooKeeper service that this Cruise Control service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

cruisecontrol

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: Anomaly Detection Goals

Description

Whether to suppress configuration warnings produced by the Anomaly Detection Goals configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_anomaly.detection.goals

Required

true

Suppress Configuration Validator: Anomaly Notifier Class

Description

Whether to suppress configuration warnings produced by the Anomaly Notifier Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_anomaly.notifier.class

Required

true

Suppress Configuration Validator: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for auth.credentials

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for auth.credentials configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_auth.credentials_role_safety_valve

Required

true

Suppress Configuration Validator: ADMIN Level Users

Description

Whether to suppress configuration warnings produced by the ADMIN Level Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_auth_admins

Required

true

Suppress Configuration Validator: USER Level Users

Description

Whether to suppress configuration warnings produced by the USER Level Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_auth_users

Required

true

Suppress Configuration Validator: VIEWER Level Users

Description

Whether to suppress configuration warnings produced by the VIEWER Level Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_auth_viewers

Required

true

Suppress Configuration Validator: Broker Metrics Topic

Description

Whether to suppress configuration warnings produced by the Broker Metrics Topic configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_broker.metric.sample.store.topic

Required

true

Suppress Configuration Validator: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for capacity.json

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for capacity.json configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_capacity.json_role_safety_valve

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Cruise Control Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cruise_control_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for cruisecontrol.properties

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for cruisecontrol.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cruisecontrol.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Default Goals

Description

Whether to suppress configuration warnings produced by the Default Goals configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_default.goals

Required

true

Suppress Configuration Validator: Supported Goals

Description

Whether to suppress configuration warnings produced by the Supported Goals configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_goals

Required

true

Suppress Configuration Validator: Hard Goals

Description

Whether to suppress configuration warnings produced by the Hard Goals configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hard.goals

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Cruise Control Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Cruise Control Server Log Directory

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Metric Anomaly Finder Class

Description

Whether to suppress configuration warnings produced by the Metric Anomaly Finder Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metric.anomaly.finder.class

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Partition Metrics Topic

Description

Whether to suppress configuration warnings produced by the Partition Metrics Topic configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_partition.metric.sample.store.topic

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Self-Healing Goals

Description

Whether to suppress configuration warnings produced by the Self-Healing Goals configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_self.healing.goals

Required

true

Suppress Configuration Validator: Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Cruise Control Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Cruise Control Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Cruise Control Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Cruise Control Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Cruise Control Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Cruise Control Server TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Cruise Control Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Cruise Control Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Cruise Control Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Cruise Control Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Trusted Proxy Authentication Service

Description

Whether to suppress configuration warnings produced by the Trusted Proxy Authentication Service configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_trusted_auth_service_user

Required

true

Suppress Configuration Validator: Cruise Control Webserver Port

Description

Whether to suppress configuration warnings produced by the Cruise Control Webserver Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver.http.port

Required

true

Suppress Configuration Validator: Cruise Control Server Count Validator

Description

Whether to suppress configuration warnings produced by the Cruise Control Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_cruise_control_server_count_validator

Required

true

Suppress Parameter Validation: Cruise Control Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cruise Control Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cruise_control_service_env_safety_valve

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Cruise Control Server Health

Description

Whether to suppress the results of the Cruise Control Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_cruise_control_cruise_control_cruise_control_server_health

Required

true

Data Analytics Studio Properties in Cloudera Runtime 7.2.18

Role groups:

Data Analytics Studio Eventprocessor

Advanced

Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor.properties

Description

For advanced use only. A string to be inserted into conf/props/eventprocessor.properties for this role only.

Related Name

Default Value

API Name

conf/props/eventprocessor.properties_role_safety_valve

Required

false

Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor_extra.properties

Description

For advanced use only. A string to be inserted into conf/props/eventprocessor_extra.properties for this role only.

Related Name

Default Value

API Name

conf/props/eventprocessor_extra.properties_role_safety_valve

Required

false

Data Analytics Studio Eventprocessor Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

DAS_EVENT_PROCESSOR_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

das_event_processor_fd_thresholds

Required

false

Data Analytics Studio Eventprocessor Host Health Test

Description

When computing the overall Data Analytics Studio Eventprocessor health, consider the host's health.

Related Name

Default Value

true

API Name

das_event_processor_host_health_enabled

Required

false

Data Analytics Studio Eventprocessor Process Health Test

Description

Enables the health test that the Data Analytics Studio Eventprocessor's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

das_event_processor_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Additional Eventprocessor Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags and/or extra debugging flags are set here.

Related Name

das_eventprocessor_java_opts

Default Value

-Xmx4096m

API Name

das_eventprocessor_java_opts

Required

false

Additional Eventprocessor Classpath

Description

Extra classpath arguments for eventprocessor.

Related Name

data_analytics_studio_ep_additional_classpath

Default Value

API Name

data_analytics_studio_ep_additional_classpath

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

DAS Eventprocessor Admin Port

Description

Port for eventprocessor admin endpoint

Related Name

data_analytics_studio_event_processor_admin_server_port

Default Value

30901

API Name

data_analytics_studio_event_processor_admin_server_port

Required

true

DAS Eventprocessor Port

Description

Port to eventprocessor server

Related Name

data_analytics_studio_event_processor_server_port

Default Value

30900

API Name

data_analytics_studio_event_processor_server_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Data Analytics Studio Eventprocessor TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Data Analytics Studio Eventprocessor might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

das.eventprocessor.ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Data Analytics Studio Eventprocessor TLS/SSL Trust Store Password

Description

The password for the Data Analytics Studio Eventprocessor TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

das.eventprocessor.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Data Analytics Studio Eventprocessor

Description

Encrypt communication between clients and Data Analytics Studio Eventprocessor using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

data_analytics_studio_event_processor_ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Data Analytics Studio Eventprocessor is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

data_analytics_studio_event_processor_keystore_file

Default Value

API Name

ssl_server_keystore_location

Required

false

Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Password

Description

The password for the Data Analytics Studio Eventprocessor keystore file.

Related Name

das_event_processor_keystore_password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/eventprocessor.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor_extra.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor_extra.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/eventprocessor_extra.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_event_processor_role_env_safety_valve

Required

true

Suppress Parameter Validation: Additional Eventprocessor Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Eventprocessor Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_eventprocessor_java_opts

Required

true

Suppress Parameter Validation: Additional Eventprocessor Classpath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Eventprocessor Classpath parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_ep_additional_classpath

Required

true

Suppress Parameter Validation: DAS Eventprocessor Admin Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Eventprocessor Admin Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_event_processor_admin_server_port

Required

true

Suppress Parameter Validation: DAS Eventprocessor Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Eventprocessor Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_event_processor_server_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Eventprocessor TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_event_processor_unexpected_exits

Required

true

Data Analytics Studio Webapp Server

Advanced

Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/props/webapp.properties

Description

For advanced use only. A string to be inserted into conf/props/webapp.properties for this role only.

Related Name

Default Value

API Name

conf/props/webapp.properties_role_safety_valve

Required

false

Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-audit.xml

Description

For advanced use only. A string to be inserted into conf/ranger-hive-audit.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-hive-audit.xml_role_safety_valve

Required

false

Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-hive-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-hive-policymgr-ssl.xml_role_safety_valve

Required

false

Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-security.xml

Description

For advanced use only. A string to be inserted into conf/ranger-hive-security.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-hive-security.xml_role_safety_valve

Required

false

Data Analytics Studio Webapp Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

DAS_WEBAPP_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

das_webapp_fd_thresholds

Required

false

Data Analytics Studio Webapp Server Host Health Test

Description

When computing the overall Data Analytics Studio Webapp Server health, consider the host's health.

Related Name

Default Value

true

API Name

das_webapp_host_health_enabled

Required

false

Data Analytics Studio Webapp Server Process Health Test

Description

Enables the health test that the Data Analytics Studio Webapp Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

das_webapp_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.

- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Additional Webapp Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags and/or extra debugging flags are set here.

Related Name

das_webapp_java_opts

Default Value

-Xmx4096m

API Name

das_webapp_java_opts

Required

false

LDAP Basedn

Description

LDAP basedn

Related Name

das_webapp_ldap_basedn

Default Value

API Name

das_webapp_ldap_basedn

Required

false

LDAP Custom Query

Description

LDAP custom query

Related Name

das_webapp_ldap_custom_ldap_query

Default Value

API Name

das_webapp_ldap_custom_ldap_query

Required

false

LDAP Domain

Description

LDAP domain

Related Name

das_webapp_ldap_domain

Default Value

API Name

das_webapp_ldap_domain

Required

false

LDAP Group Class Key

Description

LDAP group class key

Related Name

das_webapp_ldap_group_class_key

Default Value

API Name

das_webapp_ldap_group_class_key

Required

false

LDAP Group DN Pattern

Description

LDAP group DN pattern

Related Name

das_webapp_ldap_group_dn_pattern

Default Value

API Name

das_webapp_ldap_group_dn_pattern

Required

false

LDAP Group Filter

Description

LDAP group filter

Related Name

das_webapp_ldap_group_filter

Default Value

API Name

das_webapp_ldap_group_filter

Required

false

LDAP Group Membership Key

Description

LDAP group membership key

Related Name

das_webapp_ldap_group_membership_key

Default Value

API Name

das_webapp_ldap_group_membership_key

Required

false

LDAP GUID Key

Description

Knox LDAP GUID key

Related Name

das_webapp_ldap_guid_key

Default Value

API Name

das_webapp_ldap_guid_key

Required

false

LDAP URL

Description

Knox LDAP URL

Related Name

das_webapp_ldap_url

Default Value

API Name

das_webapp_ldap_url

Required

false

LDAP User DN Pattern

Description

LDAP user DN pattern

Related Name

das_webapp_ldap_user_dn_pattern

Default Value

API Name

das_webapp_ldap_user_dn_pattern

Required

false

LDAP User Filter

Description

LDAP user filter

Related Name

das_webapp_ldap_user_filter

Default Value

API Name

das_webapp_ldap_user_filter

Required

false

LDAP User Membership Key

Description

LDAP user membership key

Related Name

das_webapp_ldap_user_membership_key

Default Value

API Name

das_webapp_ldap_user_membership_key

Required

false

Admin Users

Description

List of comma seperator users who should have admin privileges.

Related Name

data_analytics_studio_admin_users

Default Value

API Name

data_analytics_studio_admin_users

Required

false

DAS User Authentication

Description

DAS user authentication, the value DEFAULT maps to NONE in insecure clusters and to SPNEGO in secure clusters.

Related Name

data_analytics_studio_user_authentication

Default Value

DEFAULT

API Name

data_analytics_studio_user_authentication

Required

false

Additional Webapp Classpath

Description

Additional Webapp classpath

Related Name

data_analytics_studio_webapp_additional_classpath

Default Value

API Name

data_analytics_studio_webapp_additional_classpath

Required

false

Knox Proxy doAs Param Name

Description

Knox proxy doAs param name

Related Name

data_analytics_studio_webapp_doas_param_name

Default Value

doAs

API Name

data_analytics_studio_webapp_doas_param_name

Required

false

Knox JWT Cookie Name

Description

Knox JWT cookie name

Related Name

data_analytics_studio_webapp_knox_cookiename

Default Value

hadoop-jwt

API Name

data_analytics_studio_webapp_knox_cookiename

Required

false

Knox JWT Cookie Public Key

Description

Knox JWT Cookie public key

Related Name

data_analytics_studio_webapp_knox_publickey

Default Value

API Name

data_analytics_studio_webapp_knox_publickey

Required

false

Knox SSO Endpoint

Description

Knox SSO endpoint

Related Name

data_analytics_studio_webapp_knox_sso_url

Default Value

API Name

data_analytics_studio_webapp_knox_sso_url

Required

false

Knox Logout Endpoint

Description

Knox logout endpoint

Related Name

data_analytics_studio_webapp_knox_ssout_url

Default Value

API Name

data_analytics_studio_webapp_knox_ssout_url

Required

false

Knox Redirect Url Param

Description

Knox redirect url param

Related Name

data_analytics_studio_webapp_knox_url_query_param

Default Value

originalUrl

API Name

data_analytics_studio_webapp_knox_url_query_param

Required

false

Knox SPNEGO User

Description

Knox SPNEGO user

Related Name

data_analytics_studio_webapp_knox_user

Default Value

knox

API Name

data_analytics_studio_webapp_knox_user

Required

false

Knox Useragent

Description

Knox useragent

Related Name

data_analytics_studio_webapp_knox_useragent

Default Value

Mozilla, Chrome

API Name

data_analytics_studio_webapp_knox_useragent

Required

false

Webapp Session Timeout

Description

The user session timeout in seconds.

Related Name

data_analytics_studio_webapp_session_timeout

Default Value

1 day(s)

API Name

data_analytics_studio_webapp_session_timeout

Required

false

Knox SPNEGO Name Rules

Description

Knox SPNEGO name rules

Related Name

data_analytics_studio_webapp_spnego_name_rules

Default Value

API Name

data_analytics_studio_webapp_spnego_name_rules

Required

false

Ranger Hive Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hive/audit/hdfs/spool

API Name

ranger_hive_plugin_hdfs_audit_spool_directory

Required

true

Ranger Hive Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hive.policy.cache.dir

Default Value

/var/lib/ranger/hive/policy-cache

API Name

ranger_hive_plugin_policy_cache_directory

Required

true

Ranger Hive Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hive/audit/solr/spool

API Name

ranger_hive_plugin_solr_audit_spool_directory

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

DAS Webapp Admin Port

Description

Port for webapp admin endpoints

Related Name

data_analytics_studio_webapp_admin_port

Default Value

30801

API Name

data_analytics_studio_webapp_admin_port

Required

true

DAS Webapp Port

Description

Port to access the DAS UI

Related Name

data_analytics_studio_webapp_server_port

Default Value

30800

API Name

data_analytics_studio_webapp_server_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Data Analytics Studio Webapp Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Data Analytics Studio Webapp Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

das.webapp.ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Data Analytics Studio Webapp Server TLS/SSL Trust Store Password

Description

The password for the Data Analytics Studio Webapp Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

das.webapp.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Data Analytics Studio Webapp Server

Description

Encrypt communication between clients and Data Analytics Studio Webapp Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

data_analytics_studio_webapp_ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Data Analytics Studio Webapp Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

data_analytics_studio_webapp_keystore_file

Default Value

API Name

ssl_server_keystore_location

Required

false

Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Password

Description

The password for the Data Analytics Studio Webapp Server keystore file.

Related Name

das_webapp_keystore_password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/props/webapp.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/props/webapp.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/webapp.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Additional Webapp Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Webapp Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_java_opts

Required

true

Suppress Parameter Validation: LDAP Basedn

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Basedn parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_basedn

Required

true

Suppress Parameter Validation: LDAP Custom Query

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Custom Query parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_custom_ldap_query

Required

true

Suppress Parameter Validation: LDAP Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Domain parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_domain

Required

true

Suppress Parameter Validation: LDAP Group Class Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Class Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_class_key

Required

true

Suppress Parameter Validation: LDAP Group DN Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group DN Pattern parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_dn_pattern

Required

true

Suppress Parameter Validation: LDAP Group Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_filter

Required

true

Suppress Parameter Validation: LDAP Group Membership Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Membership Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_membership_key

Required

true

Suppress Parameter Validation: LDAP GUID Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP GUID Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_guid_key

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_url

Required

true

Suppress Parameter Validation: LDAP User DN Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User DN Pattern parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_dn_pattern

Required

true

Suppress Parameter Validation: LDAP User Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_filter

Required

true

Suppress Parameter Validation: LDAP User Membership Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Membership Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_membership_key

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_role_env_safety_valve

Required

true

Suppress Parameter Validation: Admin Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_admin_users

Required

true

Suppress Parameter Validation: Additional Webapp Classpath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Webapp Classpath parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_additional_classpath

Required

true

Suppress Parameter Validation: DAS Webapp Admin Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Webapp Admin Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_admin_port

Required

true

Suppress Parameter Validation: Knox Proxy doAs Param Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy doAs Param Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_doas_param_name

Required

true

Suppress Parameter Validation: Knox JWT Cookie Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox JWT Cookie Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_cookiename

Required

true

Suppress Parameter Validation: Knox JWT Cookie Public Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox JWT Cookie Public Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_publickey

Required

true

Suppress Parameter Validation: Knox SSO Endpoint

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SSO Endpoint parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_sso_url

Required

true

Suppress Parameter Validation: Knox Logout Endpoint

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Logout Endpoint parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_ssout_url

Required

true

Suppress Parameter Validation: Knox Redirect Url Param

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Redirect Url Param parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_url_query_param

Required

true

Suppress Parameter Validation: Knox SPNEGO User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SPNEGO User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_user

Required

true

Suppress Parameter Validation: Knox Useragent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Useragent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_useragent

Required

true

Suppress Parameter Validation: DAS Webapp Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Webapp Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_server_port

Required

true

Suppress Parameter Validation: Knox SPNEGO Name Rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox SPNEGO Name Rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_spnego_name_rules

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ranger Hive Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Hive Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Hive Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Hive Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Hive Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Hive Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_das_das_webapp_unexpected_exits

Required

true

Service-Wide

Advanced

Data Analytics Studio Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

DAS_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_username

Required

true

Database

DAS Database Hostname

Description

Name of the host where the database is running.

Related Name

data_analytics_studio_database_host

Default Value

localhost

API Name

data_analytics_studio_database_host

Required

true

DAS Database Name

Description

DAS database name.

Related Name

data_analytics_studio_database_name

Default Value

das

API Name

data_analytics_studio_database_name

Required

true

DAS Database Password

Description

DAS database password.

Related Name

data_analytics_studio_database_password

Default Value

API Name

data_analytics_studio_database_password

Required

true

DAS Database Port

Description

DAS database port.

Related Name

data_analytics_studio_database_port

Default Value

5432

API Name

data_analytics_studio_database_port

Required

true

DAS Database Type

Description

Database type.

Related Name

data_analytics_studio_database_type

Default Value

postgresql

API Name

data_analytics_studio_database_type

Required

true

DAS Database Username

Description

DAS database username

Related Name

data_analytics_studio_database_username

Default Value

das

API Name

data_analytics_studio_database_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Application Connector Configurations

Description

Extra configurations that can be added into Dropwizard applicationConnector.

Related Name

das_application_connector_configs

Default Value

API Name

das_application_connector_configs

Required

false

Hive Secure Session Parameters

Description

Hive session parameters which can contain password, stored securely and appended to session parameters.

Related Name

das_hive_secure_session_params

Default Value

API Name

das_hive_secure_session_params

Required

false

Hive Session Parameters

Description

Any valid session parameters for Hive: Ex: truststore when using SSL, keystore for two way ssl, protocol, ...

Related Name

das_hive_session_params

Default Value

API Name

das_hive_session_params

Required

false

DAS Database URL Query Parameters

Description

Must be a standard URL string of query parameters starting with a ? symbol

Related Name

data_analytics_studio_database_url_query_params

Default Value

API Name

data_analytics_studio_database_url_query_params

Required

false

HS2 Service

Description

Name of the HS2 service that this Data Analytics Studio service instance depends on

Related Name

Default Value

API Name

hs2_service

Required

true

Enable Kerberos Authentication

Description

Boolean flag indicating whether the Hadoop cluster is secured with Kerberos.

Related Name

kerberos.auth.enabled

Default Value

false

API Name

kerberos.auth.enabled

Required

false

Ranger Hive Plugin Hdfs Audit Directory

Description

The HDFS path on which Ranger audits are written.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hive

API Name

ranger_hive_plugin_hdfs_audit_directory

Required

false

RANGER Service

Description

Name of the RANGER service that this Data Analytics Studio service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

TEZ Service

Description

Name of the TEZ service that this Data Analytics Studio service instance depends on

Related Name

Default Value

API Name

tez_service

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor.properties

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/eventprocessor.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor_extra.properties

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Eventprocessor Advanced Configuration Snippet (Safety Valve) for conf/props/eventprocessor_extra.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/eventprocessor_extra.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/props/webapp.properties

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/props/webapp.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/props/webapp.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-audit.xml

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-security.xml

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-hive-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-hive-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Eventprocessor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Eventprocessor Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_event_processor_role_env_safety_valve

Required

true

Suppress Configuration Validator: Additional Eventprocessor Java Options

Description

Whether to suppress configuration warnings produced by the Additional Eventprocessor Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_eventprocessor_java_opts

Required

true

Suppress Configuration Validator: Additional Webapp Java Options

Description

Whether to suppress configuration warnings produced by the Additional Webapp Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_java_opts

Required

true

Suppress Configuration Validator: LDAP Basedn

Description

Whether to suppress configuration warnings produced by the LDAP Basedn configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_basedn

Required

true

Suppress Configuration Validator: LDAP Custom Query

Description

Whether to suppress configuration warnings produced by the LDAP Custom Query configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_custom_ldap_query

Required

true

Suppress Configuration Validator: LDAP Domain

Description

Whether to suppress configuration warnings produced by the LDAP Domain configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_domain

Required

true

Suppress Configuration Validator: LDAP Group Class Key

Description

Whether to suppress configuration warnings produced by the LDAP Group Class Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_class_key

Required

true

Suppress Configuration Validator: LDAP Group DN Pattern

Description

Whether to suppress configuration warnings produced by the LDAP Group DN Pattern configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_dn_pattern

Required

true

Suppress Configuration Validator: LDAP Group Filter

Description

Whether to suppress configuration warnings produced by the LDAP Group Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_filter

Required

true

Suppress Configuration Validator: LDAP Group Membership Key

Description

Whether to suppress configuration warnings produced by the LDAP Group Membership Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_group_membership_key

Required

true

Suppress Configuration Validator: LDAP GUID Key

Description

Whether to suppress configuration warnings produced by the LDAP GUID Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_guid_key

Required

true

Suppress Configuration Validator: LDAP URL

Description

Whether to suppress configuration warnings produced by the LDAP URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_url

Required

true

Suppress Configuration Validator: LDAP User DN Pattern

Description

Whether to suppress configuration warnings produced by the LDAP User DN Pattern configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_dn_pattern

Required

true

Suppress Configuration Validator: LDAP User Filter

Description

Whether to suppress configuration warnings produced by the LDAP User Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_filter

Required

true

Suppress Configuration Validator: LDAP User Membership Key

Description

Whether to suppress configuration warnings produced by the LDAP User Membership Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_ldap_user_membership_key

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_das_webapp_role_env_safety_valve

Required

true

Suppress Configuration Validator: Admin Users

Description

Whether to suppress configuration warnings produced by the Admin Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_admin_users

Required

true

Suppress Configuration Validator: Additional Eventprocessor Classpath

Description

Whether to suppress configuration warnings produced by the Additional Eventprocessor Classpath configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_ep_additional_classpath

Required

true

Suppress Configuration Validator: DAS Eventprocessor Admin Port

Description

Whether to suppress configuration warnings produced by the DAS Eventprocessor Admin Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_event_processor_admin_server_port

Required

true

Suppress Configuration Validator: DAS Eventprocessor Port

Description

Whether to suppress configuration warnings produced by the DAS Eventprocessor Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_event_processor_server_port

Required

true

Suppress Configuration Validator: Additional Webapp Classpath

Description

Whether to suppress configuration warnings produced by the Additional Webapp Classpath configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_additional_classpath

Required

true

Suppress Configuration Validator: DAS Webapp Admin Port

Description

Whether to suppress configuration warnings produced by the DAS Webapp Admin Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_admin_port

Required

true

Suppress Configuration Validator: Knox Proxy doAs Param Name

Description

Whether to suppress configuration warnings produced by the Knox Proxy doAs Param Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_doas_param_name

Required

true

Suppress Configuration Validator: Knox JWT Cookie Name

Description

Whether to suppress configuration warnings produced by the Knox JWT Cookie Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_cookiename

Required

true

Suppress Configuration Validator: Knox JWT Cookie Public Key

Description

Whether to suppress configuration warnings produced by the Knox JWT Cookie Public Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_publickey

Required

true

Suppress Configuration Validator: Knox SSO Endpoint

Description

Whether to suppress configuration warnings produced by the Knox SSO Endpoint configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_sso_url

Required

true

Suppress Configuration Validator: Knox Logout Endpoint

Description

Whether to suppress configuration warnings produced by the Knox Logout Endpoint configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_ssout_url

Required

true

Suppress Configuration Validator: Knox Redirect Url Param

Description

Whether to suppress configuration warnings produced by the Knox Redirect Url Param configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_url_query_param

Required

true

Suppress Configuration Validator: Knox SPNEGO User

Description

Whether to suppress configuration warnings produced by the Knox SPNEGO User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_user

Required

true

Suppress Configuration Validator: Knox Useragent

Description

Whether to suppress configuration warnings produced by the Knox Useragent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_knox_useragent

Required

true

Suppress Configuration Validator: DAS Webapp Port

Description

Whether to suppress configuration warnings produced by the DAS Webapp Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_server_port

Required

true

Suppress Configuration Validator: Knox SPNEGO Name Rules

Description

Whether to suppress configuration warnings produced by the Knox SPNEGO Name Rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_analytics_studio_webapp_spnego_name_rules

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ranger Hive Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Hive Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Hive Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Hive Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Hive Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Hive Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_hive_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Application Connector Configurations

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Application Connector Configurations parameter.

Related Name

Default Value

false

API Name

service_config_suppression_das_application_connector_configs

Required

true

Suppress Configuration Validator: Data Analytics Studio Eventprocessor Count Validator

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Eventprocessor Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_das_event_processor_count_validator

Required

true

Suppress Parameter Validation: Hive Secure Session Parameters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Secure Session Parameters parameter.

Related Name

Default Value

false

API Name

service_config_suppression_das_hive_secure_session_params

Required

true

Suppress Parameter Validation: Hive Session Parameters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Session Parameters parameter.

Related Name

Default Value

false

API Name

service_config_suppression_das_hive_session_params

Required

true

Suppress Parameter Validation: Data Analytics Studio Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Analytics Studio Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_das_service_env_safety_valve

Required

true

Suppress Configuration Validator: Data Analytics Studio Webapp Server Count Validator

Description

Whether to suppress configuration warnings produced by the Data Analytics Studio Webapp Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_das_webapp_count_validator

Required

true

Suppress Parameter Validation: DAS Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database Hostname parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_host

Required

true

Suppress Parameter Validation: DAS Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_name

Required

true

Suppress Parameter Validation: DAS Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_password

Required

true

Suppress Parameter Validation: DAS Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_port

Required

true

Suppress Parameter Validation: DAS Database URL Query Parameters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database URL Query Parameters parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_url_query_params

Required

true

Suppress Parameter Validation: DAS Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAS Database Username parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_analytics_studio_database_username

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Hive Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Hive Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_hive_plugin_hdfs_audit_directory

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Data Context Connector Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hive

API Name

client_config_root_dir

Required

true

Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for hive-site.xml.

Related Name

Default Value

API Name

hive_client_config_safety_valve

Required

false

Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hive-env.sh

Related Name

Default Value

API Name

hive_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

hive_client_java_opts

Required

false

Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server. Consider increasing this if you have tables with a lot of metadata and see timeout errors. Used by most Hive Metastore clients such as Hive CLI and HiveServer2, but not by Impala. Impala has a separately configured timeout.

Related Name

hive.metastore.client.socket.timeout

Default Value

5 minute(s)

API Name

hive_metastore_timeout

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

2 GiB

API Name

hive_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Service-Wide

Advanced

Data Context Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

DATA_CONTEXT_CONNECTOR_service_env_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Configuration Validator: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Data Context Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Context Connector Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_data_context_connector_service_env_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Flink Properties in Cloudera Runtime 7.2.18

Role groups:

Flink Dashboard

Advanced

Flink Dashboard Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

For advanced use only. A string to be inserted into flink-conf/flink-conf.yaml for this role only.

Related Name

Default Value

API Name

flink-conf/flink-conf.yaml_role_safety_valve

Required

false

Flink Dashboard Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

FLINK_HISTORY_SERVER_role_env_safety_valve

Required

false

Flink Dashboard Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value
20

API Name
process_start_secs

Required
false

Logs

Flink Dashboard Log Directory

Description
The log directory for log files of the role Flink Dashboard.

Related Name
log.dir

Default Value
/var/log/flink

API Name
log_dir

Required
false

Flink Dashboard Logging Threshold

Description
The minimum log level for Flink Dashboard logs

Related Name

Default Value
INFO

API Name
log_threshold

Required
false

Flink Dashboard Maximum Log File Backups

Description
The maximum number of rolled log files to keep for Flink Dashboard logs. Typically used by log4j or logback.

Related Name

Default Value
10

API Name
max_log_backup_index

Required
false

Flink Dashboard Max Log Size

Description

The maximum size, in megabytes, per log file for Flink Dashboard logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

flink_history_server_fd_thresholds

Required

false

Flink Dashboard Host Health Test

Description

When computing the overall Flink Dashboard health, consider the host's health.

Related Name

Default Value

true

API Name

flink_history_server_host_health_enabled

Required

false

Flink Dashboard Process Health Test

Description

Enables the health test that the Flink Dashboard's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

flink_history_server_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

History Server Archive Directory (HDFS)

Description

Comma separated list of directories to monitor for completed jobs.

Related Name

historyserver.archive.fs.dir

Default Value

/user/flink/applicationHistory

API Name

historyserver_archive_fs_dir

Required

true

History Server Archive Directory Refresh Interval

Description

Interval in milliseconds for refreshing the archived job directories.

Related Name

historyserver.archive.fs.refresh-interval

Default Value

10000

API Name

historyserver_archive_fs_refresh_interval

Required

true

History Server Archive Retained Jobs

Description

The maximum number of jobs to retain in each archive directory.

Related Name

historyserver.archive.retained-jobs

Default Value

50

API Name

historyserver_archive_retained_jobs

Required

true

Flink Dashboard Cluster Fetcher

Description

Flink Dashboard Cluster Fetcher

Related Name

historyserver.cluster.fetcher

Default Value

YARN

API Name

historyserver_cluster_fetcher

Required

true

Use SPNEGO Authentication

Description

Enables SPNEGO authentication.

Related Name

historyserver.security.spnego.auth.enabled

Default Value

false

API Name

historyserver_security_spnego_auth_enabled

Required

true

Kerberos Login Keytab

Description

Absolute path to a Kerberos keytab file that contains the user credentials.

Related Name

security.kerberos.login.keytab

Default Value

flink.keytab

API Name

security_kerberos_login_keytab

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Flink Dashboard Port

Description

Port of the Flink Dashboard's web interface.

Related Name

historyserver.web.port

Default Value

18211

API Name

historyserver_web_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Flink Dashboard TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Flink Dashboard might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

security.ssl.rest.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Flink Dashboard TLS/SSL Trust Store Password

Description

The password for the Flink Dashboard TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

security.ssl.rest.truststore-password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Flink Dashboard

Description

Encrypt communication between clients and Flink Dashboard using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Flink Dashboard TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Flink Dashboard is acting as a TLS/SSL server.

Related Name

security.ssl.rest.key-password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Flink Dashboard TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Flink Dashboard is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

security.ssl.rest.keystore

Default Value

API Name

ssl_server_keystore_location

Required

false

Flink Dashboard TLS/SSL Server Keystore File Password

Description

The password for the Flink Dashboard keystore file.

Related Name

security.ssl.rest.keystore-password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Flink Dashboard Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/flink-conf.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Flink Dashboard Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink_history_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: History Server Archive Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Archive Directory (HDFS) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_historyserver_archive_fs_dir

Required

true

Suppress Parameter Validation: Flink Dashboard Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_historyserver_web_port

Required

true

Suppress Parameter Validation: Flink Dashboard Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Flink Dashboard Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Kerberos Login Keytab

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Login Keytab parameter.

Related Name

Default Value

false

API Name

role_config_suppression_security_kerberos_login_keytab

Required

true

Suppress Parameter Validation: Flink Dashboard TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Flink Dashboard TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Flink Dashboard TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Flink Dashboard TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Flink Dashboard TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Dashboard TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_flink_flink_history_server_unexpected_exits

Required

true

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/flink

API Name

client_config_root_dir

Required

true

Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/atlas-application.properties

Description

For advanced use only, a string to be inserted into the client configuration for flink-conf/atlas-application.properties.

Related Name

Default Value

API Name

flink-conf/atlas-application.properties_client_config_safety_valve

Required

false

Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

For advanced use only, a string to be inserted into the client configuration for flink-conf/flink-conf.yaml.

Related Name

Default Value

API Name

flink-conf/flink-conf.yaml_client_config_safety_valve

Required

false

Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j-cli.properties

Description

For advanced use only, a string to be inserted into the client configuration for flink-conf/log4j-cli.properties.

Related Name

Default Value

API Name

flink-conf/log4j-cli.properties_client_config_safety_valve

Required

false

Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j.properties

Description

For advanced use only, a string to be inserted into the client configuration for flink-conf/log4j.properties.

Related Name

Default Value

API Name

flink-conf/log4j.properties_client_config_safety_valve

Required

false

Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/sql-client-defaults.yaml

Description

For advanced use only, a string to be inserted into the client configuration for flink-conf/sql-client-defaults.yaml.

Related Name

Default Value

API Name

flink-conf/sql-client-defaults.yaml_client_config_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Security

Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

security.ssl.rest.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Gateway TLS/SSL Trust Store Password

Description

The password for the Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

security.ssl.rest.truststore-password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/atlas-application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/atlas-application.properties_client_config_safety_valve

Required

true

Suppress Parameter Validation: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/flink-conf.yaml_client_config_safety_valve

Required

true

Suppress Parameter Validation: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j-cli.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j-cli.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/log4j-cli.properties_client_config_safety_valve

Required

true

Suppress Parameter Validation: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/log4j.properties_client_config_safety_valve

Required

true

Suppress Parameter Validation: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/sql-client-defaults.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/sql-client-defaults.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/sql-client-defaults.yaml_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Service-Wide

Advanced

Flink Service Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

For advanced use only, a string to be inserted into flink-conf/flink-conf.yaml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

flink-conf/flink-conf.yaml_service_safety_valve

Required

false

Flink Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

FLINK_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

flink

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

flink

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Enable Atlas Metadata Collection

Description

When enabling this make sure that your Flink gateway nodes also have the Atlas gateway role assigned.

Related Name

atlas.collection.enabled

Default Value

false

API Name

atlas_collection_enabled

Required

false

Atlas Metadata Namespace

Description

Metadata Namespace used in Atlas for Flink applications.

Related Name

atlas.metadata.namespace

Default Value

cm

API Name

atlas_metadata_namespace

Required

true

ATLAS Service

Description

Name of the ATLAS service that this Flink service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Checkpointing Interval (milliseconds)

Description

Gets the interval in which checkpoints are periodically scheduled. This setting defines the base interval. Checkpoint triggering may be delayed by the settings execution.checkpointing.max-concurrent-checkpoints and execution.checkpointing.min-pause

Related Name

execution.checkpointing.interval

Default Value

API Name

checkpointing_interval

Required

false

Min Pause Between Checkpoints (milliseconds)

Description

The minimal pause between checkpointing attempts. This setting defines how soon thecheckpoint coordinator may trigger another checkpoint after it becomes possible to triggeranother checkpoint with respect to the maximum number of concurrent checkpoints(see execution.checkpointing.max-concurrent-checkpoints).

Related Name

execution.checkpointing.min-pause

Default Value

0

API Name

checkpointing_min_pause

Required

true

Checkpointing Mode

Description

The checkpointing mode (exactly-once vs. at-least-once).

Related Name

execution.checkpointing.mode

Default Value

EXACTLY_ONCE

API Name

checkpointing_mode

Required

true

Checkpointing Timeout (milliseconds)

Description

The maximum time that a checkpoint may take before being discarded.

Related Name

execution.checkpointing.timeout

Default Value

60000

API Name

checkpointing_timeout

Required

true

Enable Hive Catalog for SQL Client

Description

Enables Hive Catalog for SQL Client

Related Name

enable_hive_catalog

Default Value

false

API Name

enable_hive_catalog

Required

false

JobManager JVM Options

Description

Java options to start the JVM of the JobManager with.

Related Name

env.java.opts.jobmanager

Default Value

API Name

env_java_opts_jobmanager

Required

false

TaskManager JVM Options

Description

Java options to start the JVM of the TaskManager with.

Related Name

env.java.opts.taskmanager

Default Value

API Name

env_java_opts_taskmanager

Required

false

Executor

Description

The name of the executor to be used for executing the given job.

Related Name

execution.target

Default Value

yarn-per-job

API Name

execution.target

Required

true

Network Buffer Timeout (milliseconds)

Description

The maximum time frequency (ms) for the flushing of the output buffers. By default the output buffers flush frequently to provide low latency and to aid smooth developer experience.

Related Name

execution.buffer-timeout

Default Value

100

API Name

execution_buffer_timeout

Required

true

Enable Checkpoint Compression

Description

Tells if we should use compression for the state snapshot data or not.

Related Name

execution.checkpointing.snapshot-compression

Default Value

false

API Name

execution_snapshot_compression

Required

true

Externalized Checkpoint Retention

Description

The mode defines how an externalized checkpoint should be cleaned up on job cancellation. If you choose to retain externalized checkpoints on cancellation you have to handle checkpoint clean up manually when you cancel the job as well

Related Name

execution.checkpointing.externalized-checkpoint-retention

Default Value

RETAIN_ON_CANCELLATION

API Name

externalized_checkpoint_retention

Required

true

HDFS Service

Description

Name of the HDFS service that this Flink service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

High Availability Service

Description

Defines high-availability mode used for the cluster execution. To enable high-availability, set this mode to 'ZOOKEEPER' or specify FQN of factory class.

Related Name

high-availability

Default Value

ZOOKEEPER

API Name

high_availability

Required

false

High Availability Storage Directory

Description

File system path (URI) where Flink persists metadata in high-availability setups. After changing this location please execute the `Create HA Directory` action of the Flink service.

Related Name

high-availability.storageDir

Default Value

/user/flink/ha

API Name

high_availability_storage_dir

Required

false

High Availability Zookeeper client ACL

Description

Defines the ACL (open|creator) to be configured on ZK node. The configuration value can be set to 'creator' if the ZooKeeper server configuration has the 'authProvider' property mapped to use SASLAuthenticationProvider and the cluster is configured to run in secure mode (Kerberos).

Related Name

high-availability.zookeeper.client.acl

Default Value

open

API Name

high_availability_zookeeper_client_acl

Required

false

CLI global dashboard fallback

Description

Allow the CLI to fall back to the global dashboard endpoint to access Flink jobs when the jobmanager address or yarn appId are not defined.

Related Name

historyserver.cli.fallback

Default Value

true

API Name

historyserver_cli_fallback

Required

false

Hive Service

Description

Name of the Hive service that this Flink service instance depends on

Related Name

Default Value

API Name

hive_service

Required

false

JobManager Archive Directory (HDFS)

Description

Directory to upload completed jobs to. (Add this directory to the list of monitored directories of the HistoryServer as well.) After changing this location please execute the `Create JobManager Archive Directory` action of the Flink service.

Related Name

jobmanager.archive.fs.dir

Default Value

/user/flink/applicationHistory

API Name

jobmanager_archive_fs_dir

Required

true

JobManager Heap Size

Description

JVM heap size for the JobManager

Related Name

jobmanager.heap.size

Default Value

1 GiB

API Name

jobmanager_heap_size

Required

true

Enable user specific archive subdirectory

Description

Boolean flag indicating whether the job archive should be written to a user specific subdirectory.

Related Name

jobmanager.archive.per-user

Default Value

true

API Name

jobmanager_per_user_archive

Required

false

Enable Kerberos Authentication

Description

Enables Kerberos authentication for Flink

Related Name

kerberos.auth.enabled

Default Value

false

API Name

kerberos.auth.enabled

Required

false

Max Concurrent Checkpoints

Description

The maximum number of checkpoint attempts that may be in progress at the same time. If this value is n, then no checkpoints will be triggered while n checkpoint attempts are currently in flight. For the next checkpoint to be triggered, one checkpoint attempt would need to finish or expire.

Related Name

execution.checkpointing.max-concurrent-checkpoints

Default Value

1

API Name

max_concurrent_checkpoints

Required

true

Default Parallelism

Description

Default parallelism for jobs

Related Name

parallelism.default

Default Value

1

API Name

parallelism_default

Required

true

Automatic Watermark Interval (milliseconds)

Description

The interval of the automatic watermark emission. Watermarks are used throughout the streaming system to keep track of the progress of time. They are used, for example, for time based windowing.

Related Name

pipeline.auto-watermark-interval

Default Value

200

API Name

pipeline_auto_watermark_interval

Required

true

Allow Generic Types

Description

If the use of generic types is disabled, Flink will throw an UnsupportedOperationException whenever it encounters a data type that would go through Kryo for serialization.

Related Name

pipeline.generic-types

Default Value

true

API Name

pipeline_generic_types

Required

true

Max Parallelism

Description

The program-wide maximum parallelism used for operators which haven't specified a maximum parallelism. The maximum parallelism specifies the upper limit for dynamic scaling and the number of key groups used for partitioned state.

Related Name

pipeline.max-parallelism

Default Value

API Name

pipeline_max_parallelism

Required

false

Enable Object Reuse

Description

When enabled objects that Flink internally uses for deserialization and passing data to user-code functions will be reused. Keep in mind that this can lead to bugs when the user-code function of an operation is not aware of this behaviour.

Related Name

pipeline.object-reuse

Default Value

false

API Name

pipeline_object_reuse

Required

true

Kerberos Login Contexts

Description

A comma-separated list of login contexts to provide the Kerberos credentials to (for example, `Client,KafkaClient` to use the credentials for ZooKeeper authentication and for Kafka authentication)

Related Name

security.kerberos.login.contexts

Default Value

Client KafkaClient RegistryClient

API Name

security_kerberos_login_contexts

Required

false

Kerberos Use Ticket Cache

Description

Indicates whether to read from your Kerberos ticket cache.

Related Name

security.kerberos.login.use-ticket-cache

Default Value

true

API Name

security_kerberos_login_use_ticket_cache

Required

false

Catalog for SQL Client

Description

Catalog for SQL Client

Related Name

sql_current_catalog

Default Value

MEMORY

API Name

sql_current_catalog

Required

true

SQL Client Current Database

Description

SQL Client Current Database

Related Name

sql_current_db

Default Value

API Name

sql_current_db

Required

false

State Backend

Description

The state backend to be used to store and checkpoint state.

Related Name

state.backend

Default Value

FILESYSTEM

API Name

state_backend

Required

false

Incremental Checkpoints

Description

Option whether the state backend should create incremental checkpoints, if possible. For an incremental checkpoint, only a diff from the previous checkpoint is stored, rather than the complete checkpoint state. Some state backends may not support incremental checkpoints and ignore this option.

Related Name

state.backend.incremental

Default Value

true

API Name

state_backend_incremental

Required

true

Local State Recovery

Description

This option configures local recovery for this state backend. By default, local recovery is deactivated. Local recovery currently only covers keyed state backends. Currently, MemoryStateBackend does not support local recovery and ignore this option.

Related Name

state.backend.local-recovery

Default Value

true

API Name

state_backend_local_recovery

Required

true

RocksDB High-Prio Memory Fraction

Description

The fraction of cache memory that is reserved for high-priority data like index, filter, and compression dictionary blocks. This option only has an effect when 'state.backend.rocksdb.memory.managed' or 'state.backend.rocksdb.memory.fixed-per-slot' are configured.

Related Name

state.backend.rocksdb.memory.high-prio-pool-ratio

Default Value

0.1

API Name

state_backend_rocksdb_memory_high_prio_ratio

Required

true

RocksDB Memory Management

Description

If set, the RocksDB state backend will automatically configure itself to use the managed memory budget of the task slot, and divide the memory over write buffers, indexes, block caches, etc. That way, the three major uses of memory of RocksDB will be capped.

Related Name

state.backend.rocksdb.memory.managed

Default Value

true

API Name

state_backend_rocksdb_memory_managed

Required

true

RocksDB Write Buffer Memory Fraction

Description

The maximum amount of memory that write buffers may take, as a fraction of the total shared memory. This option only has an effect when 'state.backend.rocksdb.memory.managed' or 'state.backend.rocksdb.memory.fixed-per-slot' are configured.

Related Name

state.backend.rocksdb.memory.write-buffer-ratio

Default Value

0.5

API Name

state_backend_rocksdb_memory_write_buffer_ratio

Required

true

Predefined options for RocksDB state backend

Description

The predefined settings for RocksDB DBOptions and ColumnFamilyOptions by Flink community. Current supported candidate predefined-options are DEFAULT, SPINNING_DISK_OPTIMIZED, SPINNING_DISK_OPTIMIZED_HIGH_MEM or FLASH_SSD_OPTIMIZED. Note that user customized options and options from the RocksDBOptionsFactory are applied on top of these predefined ones.

Related Name

state.backend.rocksdb.predefined-options

Default Value

DEFAULT

API Name

state_backend_rocksdb_predefined_options

Required

true

RocksDB StateBackend Timer Service Factory

Description

This determines the factory for timer service state implementation. Options are either HEAP (heap-based, default) or ROCKSDB for an implementation based on RocksDB.

Related Name

state.backend.rocksdb.timer-service.factory

Default Value

ROCKSDB

API Name

state_backend_rocksdb_timer_service_factory

Required

true

State Checkpoints Directory (HDFS)

Description

The default directory used for storing the data files and meta data of checkpoints in a Flink supported filesystem. After changing this location please execute the `Create State Checkpoint Directory` action of the Flink service.

Related Name

state.checkpoints.dir

Default Value

/user/flink/checkpoints

API Name

state_checkpoints_dir

Required

false

Number of Checkpoints to Retain

Description

The maximum number of completed checkpoints to retain.

Related Name

state.checkpoints.num-retained

Default Value

3

API Name

state_checkpoints_num_retained

Required

false

State Savepoints Directory (HDFS)

Description

The default directory used for storing the data files and meta data of checkpoints in a Flink supported filesystem. After changing this location please execute the `Create State Savepoint Directory` action of the Flink service.

Related Name

state.savepoints.dir

Default Value

/user/flink/savepoints

API Name

state_savepoints_dir

Required

false

TaskManager Managed Memory Fraction

Description

Fraction of Total Flink Memory to be used as Managed Memory, if Managed Memory size is not explicitly specified. Managed memory is used by Flink operators (caching, sorting, hashtables) and state backends (RocksDB).

Related Name

taskmanager.memory.managed.fraction

Default Value

0.4

API Name

taskmanager_managed_memory_fraction

Required

true

TaskManager Process Memory Size

Description

This includes all the memory that a TaskExecutor consumes, consisting of Total Flink Memory, JVM Metaspace, and JVM Overhead. On containerized setups, this should be set to the container memory. See also 'taskmanager.memory.flink.size' for total Flink memory size configuration.

Related Name

taskmanager.memory.process.size

Default Value

2 GiB

API Name

taskmanager_memory_process_size

Required

true

Network Buffer JVM Memory Fraction

Description

Fraction of JVM memory to use for network buffers. This determines how many streaming data exchange channels a TaskManager can have at the same time and how well buffered the channels are. If a job is rejected or you get a warning that the system has not enough buffers available, increase this value or the min/max values below. Also note, that 'taskmanager.memory.network.min' and 'taskmanager.memory.network.max' may override this fraction.

Related Name

taskmanager.memory.network.fraction

Default Value

0.1

API Name

taskmanager_network_memory_fraction

Required

true

Network Buffer Memory Max

Description

Max Network Memory size for TaskExecutors. Network Memory is off-heap memory reserved for ShuffleEnvironment (e.g., network buffers). Network Memory size is derived to make up the configured fraction of the Total Flink Memory. If the derived size is less/greater than the configured min/max size, the min/max size will be used. The exact size of Network Memory can be explicitly specified by setting the min/max to the same value.

Related Name

taskmanager.memory.network.max

Default Value

2 GiB

API Name

taskmanager_network_memory_max

Required

true

TaskManager Number of Task Slots

Description

The number of parallel operator or user function instances that a single TaskManager can run. If this value is larger than 1, a single TaskManager takes multiple instances of a function or operator. That way, the TaskManager can utilize multiple CPU cores, but at the same time, the available memory is divided between the different operator or function instances. This value is typically proportional to the number of physical CPU cores that the TaskManager's machine has (e.g., equal to the number of cores, or half the number of cores).

Related Name

taskmanager.numberOfTaskSlots

Default Value

1

API Name

taskmanager_number_of_task_slots

Required

true

Maximum ApplicationMaster Attempts for YARN

Description

Number of ApplicationMaster restarts. Note that that the entire Flink cluster will restart and the YARN Client will loose the connection. Also, the JobManager address will change and you'll need to set the JM host:port manually. It is recommended to leave this option at 1.

Related Name

yarn.application-attempts

Default Value

5

API Name

yarn_application_attempts

Required

false

Maximum Failed Containers for YARN

Description

Maximum number of containers the system is going to reallocate in case of a failure.

Related Name

yarn.maximum-failed-containers

Default Value

100

API Name

yarn_maximum_failed_containers

Required

false

YARN Service

Description

Name of the YARN service that this Flink service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

YARN Tags

Description

A comma-separated list of tags to apply to the Flink YARN application.

Related Name

yarn.tags

Default Value

flink

API Name

yarn_tags

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Flink service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

flink

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/atlas-application.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/atlas-application.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

Whether to suppress configuration warnings produced by the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/flink-conf.yaml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Flink Dashboard Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/flink-conf.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j-cli.properties

Description

Whether to suppress configuration warnings produced by the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j-cli.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/log4j-cli.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j.properties

Description

Whether to suppress configuration warnings produced by the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/log4j.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/log4j.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/sql-client-defaults.yaml

Description

Whether to suppress configuration warnings produced by the Flink Client Advanced Configuration Snippet (Safety Valve) for flink-conf/sql-client-defaults.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink-conf/sql-client-defaults.yaml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Flink Dashboard Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flink_history_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: History Server Archive Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the History Server Archive Directory (HDFS) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_historyserver_archive_fs_dir

Required

true

Suppress Configuration Validator: Flink Dashboard Port

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_historyserver_web_port

Required

true

Suppress Configuration Validator: Flink Dashboard Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Flink Dashboard Log Directory

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Kerberos Login Keytab

Description

Whether to suppress configuration warnings produced by the Kerberos Login Keytab configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_security_kerberos_login_keytab

Required

true

Suppress Configuration Validator: Flink Dashboard TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Flink Dashboard TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Flink Dashboard TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Flink Dashboard TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Flink Dashboard TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Flink Dashboard TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Flink Dashboard TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Flink Dashboard TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Flink Dashboard TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Flink Dashboard TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Atlas Metadata Namespace

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Metadata Namespace parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_metadata_namespace

Required

true

Suppress Parameter Validation: JobManager JVM Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobManager JVM Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_env_java_opts_jobmanager

Required

true

Suppress Parameter Validation: TaskManager JVM Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TaskManager JVM Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_env_java_opts_taskmanager

Required

true

Suppress Parameter Validation: Flink Service Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Service Advanced Configuration Snippet (Safety Valve) for flink-conf/flink-conf.yaml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_flink-conf/flink-conf.yaml_service_safety_valve

Required

true

Suppress Configuration Validator: Flink Dashboard Count Validator

Description

Whether to suppress configuration warnings produced by the Flink Dashboard Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_flink_history_server_count_validator

Required

true

Suppress Parameter Validation: Flink Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_flink_service_env_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: High Availability Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the High Availability Storage Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_high_availability_storage_dir

Required

true

Suppress Parameter Validation: High Availability Zookeeper client ACL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the High Availability Zookeeper client ACL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_high_availability_zookeeper_client_acl

Required

true

Suppress Parameter Validation: JobManager Archive Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobManager Archive Directory (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_jobmanager_archive_fs_dir

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Kerberos Login Contexts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Login Contexts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_security_kerberos_login_contexts

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: SQL Client Current Database

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SQL Client Current Database parameter.

Related Name

Default Value

false

API Name

service_config_suppression_sql_current_db

Required

true

Suppress Parameter Validation: State Checkpoints Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the State Checkpoints Directory (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_state_checkpoints_dir

Required

true

Suppress Parameter Validation: State Savepoints Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the State Savepoints Directory (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_state_savepoints_dir

Required

true

Suppress Parameter Validation: YARN Tags

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Tags parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_tags

Required

true

GCS Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

GCS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

GCS_service_env_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Google Cloud Storage Account Name

Description

Name of an Google Cloud Storage account.

Related Name

Default Value

API Name

cloud_account

Required

true

Security

Credentials Protection Policy

Description

Determines a security policy for the distribution of Google Cloud Storage account credentials to cluster services. 'More Secure': Encrypted at all times and directly available to a limited set of services. 'Less Secure': Credentials may be in plain text in some configuration files for specific services in the cluster.

Related Name

Default Value

SECURE

API Name

key_distribution_policy

Required

true

Suppressions

Suppress Parameter Validation: GCS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the GCS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_gcs_service_env_safety_valve

Required

true

HBase Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hbase

API Name

client_config_root_dir

Required

true

HBase Client Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for hbase-site.xml.

Related Name

Default Value

API Name

hbase_client_config_safety_valve

Required

false

HBase Client Environment Advanced Configuration Snippet (Safety Valve) for hbase-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hbase-env.sh

Related Name

Default Value

API Name

hbase_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-XX:+HeapDumpOnOutOfMemoryError -Djava.net.preferIPv4Stack=true

API Name

hbase_client_java_opts

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

HBase Client Get Timeout For Secondary Region Replicas

Description

If a get operation is performed with 'Consistency.TIMELINE', the read RPC is sent to the primary RegionServer first. After this timeout, parallel RPC for secondary region replicas is also sent if the primary does not respond. After this, the result is returned from whichever RPC is finished first. If the response returns from the primary region replica, that data is the most recent. Result.isStale() API has been added to inspect the staleness. If the result is from a secondary region, Result.isStale() is set to true.

Related Name

hbase.client.primaryCallTimeout.get

Default Value

10 second(s)

API Name

hbase_client_primaryCallTimeout_get

Required

false

HBase Client Multiget Timeout For Secondary Region Replicas

Description

If a multiget operation is performed with 'Consistency.TIMELINE', the read RPC is sent to the primary RegionServer first. After this timeout, a parallel RPC for secondary region replicas is also sent if the primary does not respond. After this, the result is returned from whichever RPC is finished first. If the response returns from the primary region replica, that the data is the most recent. Result.isStale() API has been added to inspect the staleness. If the result is from a secondary region, Result.isStale() is set to true.

Related Name

hbase.client.primaryCallTimeout.multiget

Default Value

10 second(s)

API Name

hbase_client_primaryCallTimeout_multiget

Required

false

HBase Client Scanner Timeout

Description

Scanner Timeout, in milliseconds, for HBase Clients. Scanner related RPCs will apply this timeout against the RegionServers they talk to.

Related Name

hbase.client.scanner.timeout.period

Default Value

1 minute(s)

API Name

hbase_client_scanner_timeout_period

Required

false

Enable Client RPC Threads Interruption

Description

Whether to enable interruption of RPC threads at the client. The default value of true enables primary RegionServers to access data from other regions' secondary replicas.

Related Name

hbase.ipc.client.allowsInterrupt

Default Value

true

API Name

hbase_ipc_client_allowsInterrupt

Required

false

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

hbase_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: HBase Client Scanner Timeout exceeds Lease Period Validator

Description

Whether to suppress configuration warnings produced by the HBase Client Scanner Timeout exceeds Lease Period Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_server_scanner_rpc_timeout_validator

Required

true

Suppress Parameter Validation: HBase Client Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Client Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_config_safety_valve

Required

true

Suppress Parameter Validation: HBase Client Environment Advanced Configuration Snippet (Safety Valve) for hbase-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Client Environment Advanced Configuration Snippet (Safety Valve) for hbase-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

HBase REST Server

Advanced

HBase REST Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only. A string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

hbase_restserver_config_safety_valve

Required

false

Java Configuration Options for HBase REST Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hbase_restserver_java_opts

Required

false

HBase REST Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HBASERESTSERVER_role_env_safety_valve

Required

false

HBase REST Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists,

it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HBase REST Server Log Directory

Description

Directory where HBase REST Server will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hbase

API Name

hbase_restserver_log_dir

Required

false

HBase REST Server Logging Threshold

Description

The minimum log level for HBase REST Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HBase REST Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HBase REST Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HBase REST Server Max Log Size

Description

The maximum size, in megabytes, per log file for HBase REST Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hbaserestserver_fd_thresholds

Required

false

HBase REST Server Host Health Test

Description

When computing the overall HBase REST Server health, consider the host's health.

Related Name

Default Value

true

API Name

hbaserestserver_host_health_enabled

Required

false

HBase REST Server Process Health Test

Description

Enables the health test that the HBase REST Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hbaserestserver_scm_health_enabled

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: -

source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable HBase REST Server Read Only Mode

Description

When false, all HTTP methods are permitted (GET/PUT/POST/DELETE). When true, only GET is permitted.

Related Name

hbase.rest.readonly

Default Value

false

API Name

hbase_restserver_readonly

Required

false

Performance

HBase REST Server Maximum Threads

Description

Maximum size of the HBase REST Server thread pool. The server can process this number of concurrent requests. Setting this too high can lead to out of memory errors.

Related Name

hbase.rest.threads.max

Default Value

100

API Name

hbase_restserver_threads_max

Required

true

HBase REST Server Minimum Threads

Description

Minimum size of the HBase REST Server thread pool. The server will maintain at least this number of threads in the pool at all times. The thread pool can grow up to the maximum size set by hbase.rest.threads.max.

Related Name

hbase.rest.threads.min

Default Value

2

API Name

hbase_restserver_threads_min

Required

true

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

HBase REST Server DNS Network Interface

Description

The name of the DNS network interface from which an HBase REST Server should report its IP address.

Related Name

hbase.rest.dns.interface

Default Value

API Name

hbase_restserver_dns_interface

Required

false

HBase REST Server DNS Name Server

Description

The host name or IP address of the DNS name server which an HBase REST Server should use to determine the host name used for communication and display purposes.

Related Name

hbase.rest.dns.nameserver

Default Value

API Name

hbase_restserver_dns_nameserver

Required

false

HBase REST Server Host Address

Description

HBase REST Server will bind to this address.

Related Name

hbase.rest.host

Default Value

0.0.0.0

API Name

hbase_restserver_host

Required

false

HBase REST Server Web UI Bind to Wildcard Address

Description

If true, HBase REST Server Web UI will bind to a wildcard address (0.0.0.0). Otherwise it will bind to a host name. Only available in CDH 4.3 and later.

Related Name

hbase.rest.info.bindAddress

Default Value

true

API Name

hbase_restserver_info_bind_to_wildcard

Required

false

HBase REST Server Web UI Port

Description

The port that HBase REST Server Web UI binds to.

Related Name

hbase.rest.info.port

Default Value

8085

API Name

hbase_restserver_info_port

Required

true

HBase REST Server Port

Description

The port that HBase REST Server binds to.

Related Name

hbase.rest.port

Default Value

20550

API Name

hbase_restserver_port

Required

true

Resource Management

Java Heap Size of HBase REST Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

hbase_restserver_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

HBase REST Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HBase REST Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hbase.rest.ssl.keystore.store

Default Value

API Name

hbase_restserver_keystore_file

Required

false

HBase REST Server TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when HBase REST Server is acting as a TLS/SSL server.

Related Name

hbase.rest.ssl.keystore.keypassword

Default Value

API Name

hbase_restserver_keystore_keypassword

Required

false

HBase REST Server TLS/SSL Server Keystore File Password

Description

The password for the HBase REST Server keystore file.

Related Name

hbase.rest.ssl.keystore.password

Default Value

API Name

hbase_restserver_keystore_password

Required

false

Enable TLS/SSL for HBase REST Server

Description

Encrypt communication between clients and HBase REST Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hbase.rest.ssl.enabled

Default Value

false

API Name

hbase_restserver_ssl_enable

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user

with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: HBase REST Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_config_safety_valve

Required

true

Suppress Parameter Validation: HBase REST Server DNS Network Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server DNS Network Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_dns_interface

Required

true

Suppress Parameter Validation: HBase REST Server DNS Name Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server DNS Name Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_dns_nameserver

Required

true

Suppress Parameter Validation: HBase REST Server Host Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Host Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_host

Required

true

Suppress Parameter Validation: HBase REST Server Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_info_port

Required

true

Suppress Parameter Validation: Java Configuration Options for HBase REST Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HBase REST Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_java_opts

Required

true

Suppress Parameter Validation: HBase REST Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_file

Required

true

Suppress Parameter Validation: HBase REST Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_keypassword

Required

true

Suppress Parameter Validation: HBase REST Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_password

Required

true

Suppress Parameter Validation: HBase REST Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_log_dir

Required

true

Suppress Parameter Validation: HBase REST Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_port

Required

true

Suppress Parameter Validation: HBase REST Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbaserestserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: HBase REST Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase REST Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_rest_server_unexpected_exits

Required

true

HBase Thrift Server

Advanced

HBase Thrift Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only. A string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

hbase_thriftserver_config_safety_valve

Required

false

Java Configuration Options for HBase Thrift Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hbase_thriftserver_java_opts

Required

false

HBase Thrift Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HBASETHRIFTSERVER_role_env_safety_valve

Required

false

HBase Thrift Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HBase Thrift Server Log Directory

Description

Directory where HBase Thrift Server will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hbase

API Name

hbase_thriftserver_log_dir

Required

false

HBase Thrift Server Logging Threshold

Description

The minimum log level for HBase Thrift Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HBase Thrift Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HBase Thrift Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HBase Thrift Server Max Log Size

Description

The maximum size, in megabytes, per log file for HBase Thrift Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hbasethriftserver_fd_thresholds

Required

false

HBase Thrift Server Host Health Test

Description

When computing the overall HBase Thrift Server health, consider the host's health.

Related Name

Default Value

true

API Name

hbasethriftserver_host_health_enabled

Required

false

HBase Thrift Server Process Health Test

Description

Enables the health test that the HBase Thrift Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hbasethriftserver_scm_health_enabled

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".

- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable HBase Thrift Server Compact Protocol

Description

Use the TCompactProtocol instead of the default TBinaryProtocol. TCompactProtocol is a binary protocol that is more compact than the default and typically more efficient.

Related Name

hbase.regionserver.thrift.compact

Default Value

true

API Name

hbase_thriftserver_compact

Required

false

Enable HBase Thrift Server Framed Transport

Description

Use framed transport. When using the THsHaServer or TNonblockingServer, framed transport is always used irrespective of this configuration value.

Related Name

hbase.regionserver.thrift.framed

Default Value

true

API Name

hbase_thriftserver_framed

Required

false

HBase Thrift Server Type

Description

Type of HBase Thrift Server.

Related Name

hbase.regionserver.thrift.server.type

Default Value

threadpool

API Name

hbase_thriftserver_type

Required

false

Performance

HBase Thrift Server Min Worker Threads

Description

The "core size" of the thread pool. New threads are created on every connection until this many threads are created.

Related Name

hbase.thrift.minWorkerThreads

Default Value

200

API Name

hbase_thriftserver_min_worker_threads

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

HBase Thrift Server Bind Address

Description

Address to bind the HBase Thrift Server to. When using the THsHaServer or the TNonblockingServer, always binds to 0.0.0.0 irrespective of this configuration value.

Related Name

hbase.regionserver.thrift.ipaddress

Default Value

0.0.0.0

API Name

hbase_thriftserver_bindaddress

Required

false

HBase Thrift Server DNS Network Interface

Description

The name of the DNS network interface from which an HBase Thrift Server should report its IP address.

Related Name

hbase.thrift.dns.interface

Default Value

API Name

hbase_thriftserver_dns_interface

Required

false

HBase Thrift Server DNS Name Server

Description

The host name or IP address of the DNS name server which an HBase Thrift Server should use to determine the host name used for communication and display purposes.

Related Name

hbase.thrift.dns.nameserver

Default Value

API Name

hbase_thriftserver_dns_nameserver

Required

false

HBase Thrift Server Web UI Bind to Wildcard Address

Description

If true, HBase Thrift Server Web UI will bind to a wildcard address (0.0.0.0). Otherwise it will bind to a host name. Only available in CDH 4.3 and later.

Related Name

hbase.thrift.info.bindAddress

Default Value

true

API Name

hbase_thriftserver_info_bind_to_wildcard

Required

false

HBase Thrift Server Web UI Port

Description

The port that HBase Thrift Server Web UI binds to.

Related Name

hbase.thrift.info.port

Default Value

9095

API Name

hbase_thriftserver_info_port

Required

true

HBase Thrift Server Port

Description

The port that HBase Thrift Server binds to.

Related Name

hbase.regionserver.thrift.port

Default Value

9090

API Name

hbase_thriftserver_port

Required

true

Resource Management

Java Heap Size of HBase Thrift Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

hbase_thriftserver_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

HBase Thrift Server over HTTP TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HBase Thrift Server over HTTP is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hbase.thrift.ssl.keystore.store

Default Value

API Name

hbase_thriftserver_http_keystore_file

Required

false

HBase Thrift Server over HTTP TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when HBase Thrift Server over HTTP is acting as a TLS/SSL server.

Related Name

hbase.thrift.ssl.keystore.keypassword

Default Value

API Name

hbase_thriftserver_http_keystore_keypassword

Required

false

HBase Thrift Server over HTTP TLS/SSL Server Keystore File Password

Description

The password for the HBase Thrift Server over HTTP keystore file.

Related Name

hbase.thrift.ssl.keystore.password

Default Value

API Name

hbase_thriftserver_http_keystore_password

Required

false

Enable TLS/SSL for HBase Thrift Server over HTTP

Description

Encrypt communication between clients and HBase Thrift Server over HTTP using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hbase.thrift.ssl.enabled

Default Value

false

API Name

hbase_thriftserver_http_use_ssl

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: HBase Kerberos Secure Thrift Server Validator

Description

Whether to suppress configuration warnings produced by the HBase Kerberos Secure Thrift Server Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_kerberos_secure_thrift_validator

Required

true

Suppress Parameter Validation: HBase Thrift Server Bind Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Bind Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_bindaddress

Required

true

Suppress Parameter Validation: HBase Thrift Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_config_safety_valve

Required

true

Suppress Parameter Validation: HBase Thrift Server DNS Network Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server DNS Network Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_dns_interface

Required

true

Suppress Parameter Validation: HBase Thrift Server DNS Name Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server DNS Name Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_dns_nameserver

Required

true

Suppress Parameter Validation: HBase Thrift Server over HTTP TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server over HTTP TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_file

Required

true

Suppress Parameter Validation: HBase Thrift Server over HTTP TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server over HTTP TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_keypassword

Required

true

Suppress Parameter Validation: HBase Thrift Server over HTTP TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server over HTTP TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_password

Required

true

Suppress Parameter Validation: HBase Thrift Server Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_info_port

Required

true

Suppress Parameter Validation: Java Configuration Options for HBase Thrift Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HBase Thrift Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_java_opts

Required

true

Suppress Parameter Validation: HBase Thrift Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_log_dir

Required

true

Suppress Parameter Validation: HBase Thrift Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_port

Required

true

Suppress Parameter Validation: HBase Thrift Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbasethriftserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: HBase Thrift Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Thrift Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_thrift_server_unexpected_exits

Required

true

Master

Advanced

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

HBase Coprocessor Master Classes

Description

List of org.apache.hadoop.hbase.coprocessor.MasterObserver coprocessors that are loaded by default on the active HMaster process. For any implemented coprocessor methods, the listed classes will be called in order. After implementing your own MasterObserver, just put it in HBase's classpath and add the fully qualified class name here.

Related Name

hbase.coprocessor.master.classes

Default Value

API Name

hbase_coprocessor_master_classes

Required

false

Master Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only. A string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

hbase_master_config_safety_valve

Required

false

Java Configuration Options for HBase Master

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS -XX:ReservedCodeCacheSize=256m

API Name

hbase_master_java_opts

Required

false

Netty native library working directory

Description

The local working directory used for Netty native libraries.

Related Name

netty.native.workdir

Default Value

/var/hbase/netty-workdir

API Name

hbase_netty_native_workdir

Required

false

Master Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Master Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

MASTER_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Master Log Directory

Description

Directory where Master will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hbase

API Name

hbase_master_log_dir

Required

false

Master Logging Threshold

Description

The minimum log level for Master logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Master Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Master logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Master Max Log Size

Description

The maximum size, in megabytes, per log file for Master logs. Typically used by log4j or logback.

Related Name

Default Value
200 MiB

API Name
max_log_size

Required
false

Metrics

Extended Period

Description
Time period in seconds to reset long-running metrics (e.g. compactions). This is an HBase specific configuration.

Related Name
hbase.extendedperiod

Default Value
1 hour(s)

API Name
hbase_metrics_extended_period

Required
false

Monitoring

Enable Health Alerts for this Role

Description
When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value
true

API Name
enable_alerts

Required
false

Enable Configuration Change Alerts

Description
When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value
false

API Name
enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11140

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: IPC Server handler.*ClosedChannelException , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: IPC Server Responder, call.*output error , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Daughter regiondir does not exist: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: File.*might still be open.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: File.*might still be open.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Moving table .+ state to enabled but was already enabled , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Received OPENED for region.*but region was in the state.* , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Unknown job [^]+ being deleted.* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command .+ No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

HBase Master Canary Health Test

Description

Enables the health test that a client can connect to the HBase Master

Related Name

Default Value

true

API Name

master_canary_health_enabled

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

master_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

master_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

master_gc_duration_window

Required

false

Master Host Health Test

Description

When computing the overall Master health, consider the host's health.

Related Name

Default Value

true

API Name

master_host_health_enabled

Required

false

HBase Regions In Transition Over Threshold Health Test

Description

Enable the health test that checks if there are regions in transition over the threshold configured in HBase.

Related Name

Default Value

true

API Name

master_regions_in_transition_health_enabled

Required

false

Master Process Health Test

Description

Enables the health test that the Master's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

master_scm_health_enabled

Required

false

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Related Name

Default Value

5 minute(s)

API Name

master_startup_tolerance

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

master_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

master_web_metric_collection_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting

#log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HBase Master Handler Count

Description

Number of RPC Server instances spun up on HBase Master.

Related Name

hbase.master.handler.count

Default Value

25

API Name

hbase_master_handler_count

Required

false

HBase Master Log Cleaner Plugins

Description

A comma-separated list of LogCleanerDelegate(s) that are used in LogsCleaner. WAL/HLog cleaner(s) are called in order, so put the log cleaner that prunes the most log files in the front. To implement your own LogCleanerDelegate, add it to HBase's classpath and add the fully-qualified class name here. You should always add the above default log cleaners in the list, unless you have a special reason not to.

Related Name

hbase.master.logcleaner.plugins

Default Value

API Name

hbase_master_logcleaner_plugins

Required

false

Maximum Time to Keep HLogs

Description

Maximum time an HLog remains in the .oldlogdir directory until an HBase Master thread deletes it.

Related Name

hbase.master.logcleaner.ttl

Default Value

1 minute(s)

API Name

hbase_master_logcleaner_ttl

Required

false

Set HBase Master UI to read-only.

Description

Read-only mode for the HBase Master UI disallows operations from the UI which change the state of HBase, such as triggering compactions or splits.

Related Name

hbase.master.ui.readonly

Default Value

true

API Name

hbase_master_ui_readonly

Required

false

Performance

Region Closing Threads

Description

Number of pooled threads to handle region closing in the master.

Related Name

hbase.master.executor.closeregion.threads

Default Value

5

API Name

hbase_master_executor_closeregion_threads

Required

false

Region Opening Threads

Description

Number of pooled threads to handle region opening in the master.

Related Name

hbase.master.executor.openregion.threads

Default Value

5

API Name

hbase_master_executor_openregion_threads

Required

false

RegionServer Recovery Threads

Description

Number of pooled threads to handle the recovery of the RegionServers in the master.

Related Name

hbase.master.executor.serverops.threads

Default Value

5

API Name

hbase_master_executor_serverops_threads

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

HBase Master Bind to Wildcard Address

Description

When true, HBase Master will bind to 0.0.0.0. Only available with CDH 4.3 and later.

Related Name

hbase.master.ipc.address

Default Value

true

API Name

hbase_master_bind_to_wildcard_address

Required

true

HBase Master DNS Network Interface

Description

The name of the DNS network interface from which an HBase Master should report its IP address.

Related Name

hbase.master.dns.interface

Default Value

API Name

hbase_master_dns_interface

Required

false

HBase Master DNS Name Server

Description

The host name or IP address of the DNS name server which an HBase Master should use to determine the host name used for communication and display purposes.

Related Name

hbase.master.dns.nameserver

Default Value

API Name

hbase_master_dns_nameserver

Required

false

HBase Master Web UI Address

Description

The address for the HBase Master web UI

Related Name

hbase.master.info.bindAddress

Default Value

API Name

hbase_master_info_bindAddress

Required

false

HBase Master Web UI Port

Description

The port for the HBase Master web UI. Set to -1 to disable the HBase Master web UI.

Related Name

hbase.master.info.port

Default Value

16010

API Name

hbase_master_info_port

Required

false

HBase Master Port

Description

The port that the HBase Master binds to.

Related Name

hbase.master.port

Default Value

16000

API Name

hbase_master_port

Required

false

Resource Management

Java Heap Size of HBase Master in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

hbase_master_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Require EXEC privilege to execute coprocessor calls

Description

If this setting is enabled and ACL based access control is active (the AccessController coprocessor is installed either as a system coprocessor or on a table as a table coprocessor) then you must grant all relevant users EXEC privilege if they require the ability to execute coprocessor endpoint calls. EXEC privilege, like any other permission, can be granted globally to a user, or to a user on a per table or per namespace basis. For more information on coprocessor endpoints, see the coprocessor section of the HBase online manual. For more information on granting or revoking permissions using the AccessController, see the security section of the HBase online manual.

Related Name

hbase.security.exec.permission.checks

Default Value

false

API Name

hbase_security_exec_permission_checks

Required

false

HBase Master TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HBase Master might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

master_truststore_file

Required

false

HBase Master TLS/SSL Trust Store Password

Description

The password for the HBase Master TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

master_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: HBase Coprocessor Master Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Coprocessor Master Classes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_coprocessor_master_classes

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_config_safety_valve

Required

true

Suppress Parameter Validation: HBase Master DNS Network Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master DNS Network Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_dns_interface

Required

true

Suppress Parameter Validation: HBase Master DNS Name Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master DNS Name Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_dns_nameserver

Required

true

Suppress Parameter Validation: HBase Master Web UI Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master Web UI Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_info_bindaddress

Required

true

Suppress Parameter Validation: HBase Master Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_info_port

Required

true

Suppress Parameter Validation: Java Configuration Options for HBase Master

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HBase Master parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_java_opts

Required

true

Suppress Parameter Validation: Master Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_log_dir

Required

true

Suppress Parameter Validation: HBase Master Log Cleaner Plugins

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master Log Cleaner Plugins parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_logcleaner_plugins

Required

true

Suppress Parameter Validation: HBase Master Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_port

Required

true

Suppress Parameter Validation: Netty native library working directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Netty native library working directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_netty_native_workdir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Master Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Master Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_master_role_env_safety_valve

Required

true

Suppress Parameter Validation: HBase Master TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_master_truststore_file

Required

true

Suppress Parameter Validation: HBase Master TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Master TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_master_truststore_password

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_audit_health

Required

true

Suppress Health Test: HBase Master Canary

Description

Whether to suppress the results of the HBase Master Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_canary_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_otelcol_health

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: HBase Regions In Transition Over Threshold

Description

Whether to suppress the results of the HBase Regions In Transition Over Threshold heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_regions_in_transition_over_threshold

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_master_web_metric_collection

Required

true

RegionServer

Advanced

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

BucketCache IOEngine

Description

Where to store the contents of the BucketCache. Either "offheap" or file:/path/to/file -- this should be a file in the local file system (not HDFS), and is generally a file on ramdisk or SSD (not spinning disk). If this is set to "offheap" then Java's -XX:MaxDirectMemorySize is set to the value of hbase.bucketcache.size plus 1GB for short-circuit reads.

Related Name

hbase.bucketcache.ioengine

Default Value

API Name

hbase_bucketcache_ioengine

Required

false

BucketCache Size

Description

The total size of the BucketCache, in megabytes. The size to configure depends on the amount of memory available to HBase, or the size of a local SSD. If hbase.bucketcache.ioengine is set to "offheap", then the bucketcache consumes the configured amount of memory from Java's Direct Memory.

Related Name

hbase.bucketcache.size

Default Value

1 GiB

API Name

hbase_bucketcache_size

Required

false

HBase Coprocessor Region Classes

Description

List of coprocessors that are loaded by default on all tables. For any override coprocessor method, these classes will be called in order. After implementing your own coprocessor, just put it in HBase's classpath and add the fully qualified class name here. A coprocessor can also be loaded on demand by setting HTableDescriptor.

Related Name

hbase.coprocessor.region.classes

Default Value

API Name

hbase_coprocessor_region_classes

Required

false

Netty native library working directory

Description

The local working directory used for Netty native libraries.

Related Name

netty.native.workdir

Default Value

/var/hbase/netty-workdir

API Name

hbase_netty_native_workdir

Required

false

Canary Interval

Description

Duration between consecutive checks done by the Canary.

Related Name

Default Value

6 second(s)

API Name

hbase_regionserver_canary_interval

Required

false

Canary Timeout

Description

Timeout for Canary to perform its checks.

Related Name

Default Value

15 second(s)

API Name

hbase_regionserver_canary_timeout

Required

false

RegionServer Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only. A string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

hbase_regionserver_config_safety_valve

Required

false

Java Configuration Options for HBase RegionServer

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS -XX:ReservedCodeCacheSize=256m

API Name

hbase_regionserver_java_opts

Required

false

Write-Ahead Log (WAL) Codec Class

Description

Configuration key for the class to use when encoding cells in the Write-Ahead Log (WAL)

Related Name

hbase.regionserver.wal.codec

Default Value

API Name

hbase_regionserver_wal_codec

Required

false

RegionServer Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

RegionServer Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

REGIONSERVER_role_env_safety_valve

Required

false

Logs

RegionServer Log Directory

Description

Directory where RegionServer will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hbase

API Name

hbase_regionserver_log_dir

Required

false

RegionServer Logging Threshold

Description

The minimum log level for RegionServer logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

RegionServer Maximum Log File Backups

Description

The maximum number of rolled log files to keep for RegionServer logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

RegionServer Max Log Size

Description

The maximum size, in megabytes, per log file for RegionServer logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Metrics

Extended Period

Description

Time period in seconds to reset long-running metrics (e.g. compactions). This is an HBase specific configuration.

Related Name

hbase.extendedperiod

Default Value

1 hour(s)

API Name

hbase_metrics_extended_period

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11141

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics - pattern: 'Hadoop<service=HBase, name=RegionServer, sub=Server><>(pause.*): (\d+)' attrNameSnakeCase: true name: $1 value: $2 labels: hadoop_service: HBase hadoop_metric_group: region_server

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 0, threshold: WARN, content: IPC Server handler.*took.*appending an edit to hlog.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: ABORTING region server serverName.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: DFSOutputStream ResponseProcessor exception.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Error Recovery for block blk.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Failed init , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Problem renewing lease for DFSClient.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: remote error telling master we are up , alert: false, rate: 1, periodminutes: 1, threshold: WARN, content: Session.*for server.*closing socket connection and attempting reconnect. , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command .+ No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: -1, threshold: INFO, content: ^Starting .*compaction on region (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_REGION_STARTED, attribute:SEVERITY: INFORMATIONAL, group0: REGION , alert: false, rate: -1, threshold: INFO, content: ^completed compaction on region (.+) after (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_REGION_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: DURATION , alert: false, rate: -1, threshold: INFO, content: ^Starting compaction on (.+) in region (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_COLUMN_FAMILY_STARTED, attribute:SEVERITY: INFORMATIONAL, group0: COLUMN_FAMILY, group1: REGION , alert: false, rate: -1, threshold: INFO, content: ^completed compaction: regionName\u003d(.+), storeName\u003d(.+), fileCount\u003d(.+), fileSize\u003d(.+), priority\u003d(.+), time\u003d(.+); duration\u003d(.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_COLUMN_FAMILY_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: COLUMN_FAMILY, group2: FILE_COUNT, group3: FILE_SIZE, group4: PRIORITY, group5: REQUEST_TIME_NANOS, group6: DURATION , alert: false, rate: -1, threshold: INFO, content: ^Completed compaction: Request \u003d regionName\u003d(.+), storeName \u003d(.+), fileCount\u003d(.+), fileSize\u003d(.+), priority\u003d(.+), time\u003d(. +); duration\u003d(.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_COLUMN_FAMILY_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: COLUMN_FAMILY, group2: FILE_COUNT, group3: FILE_SIZE, group4: PRIORITY, group5: REQUEST_TIME_NANOS, group6: DURATION , alert: false, rate: -1, threshold: INFO, content: ^aborted compaction: regionName \u003d(.+), storeName\u003d(.+), fileCount\u003d(.+), fileSize\u003d(.+), priority\u003d(.+), time\u003d(.+); duration\u003d(.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_COMPACTION_COLUMN_FAMILY_ABORTED, attribute:SEVERITY: IMPORTANT, group0: REGION, group1: COLUMN_FAMILY, group2: FILE_COUNT, group3:

FILE_SIZE, group4: PRIORITY, group5: REQUEST_TIME_NANOS, group6: DURATION , alert: false, rate: -1, threshold: INFO, content: ^Finished memstore flush of .+ for region (.+) in (.+), sequenceid\u003d(.+), compaction requested\u003d(.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_FLUSH_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: DURATION, group2: SEQUENCE_ID, group3: COMPACTION_REQUESTED , alert: false, rate: -1, threshold: INFO, content: ^Flush of region (.+) due to global heap pressure$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_FLUSH_DUE_TO_HEAP_PRESSURE, attribute:SEVERITY: IMPORTANT, group0: REGION , alert: false, rate: -1, threshold: WARN, content: ^Region (.+) has too many store files; delaying flush up to 90000ms$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_FLUSH_DELAYED_TOO_MANY_STORE_FILES, attribute:SEVERITY: CRITICAL, group0: REGION , alert: false, rate: -1, threshold: INFO, content: ^Starting split of region (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_SPLIT_STARTED, attribute:SEVERITY: INFORMATIONAL, group0: REGION , alert: false, rate: -1, threshold: INFO, content: ^Running rollback/cleanup of failed split of (.+);.+$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_SPLIT_ABORTED, attribute:SEVERITY: IMPORTANT, group0: REGION , alert: false, rate: -1, threshold: INFO, content: ^Region split, hbase:meta updated, and report to master. Parent\u003d(.+), new regions: (.+, .*, .+), (.+, .*, .+). Split took (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_SPLIT_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: DAUGHTER_REGIONS, group2: DAUGHTER_REGIONS, group3: DURATION , alert: false, rate: -1, threshold: INFO, content: ^Region split, META updated, and report to master. Parent\u003d(.+), new regions: (.+, .*, .+), (.+, .*, .+). Split took (.+)$, attribute:CATEGORY: HBASE, attribute:EVENTCODE: EV_HBASE_SPLIT_COMPLETED, attribute:SEVERITY: INFORMATIONAL, group0: REGION, group1: DAUGHTER_REGIONS, group2: DAUGHTER_REGIONS, group3: DURATION , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes #pause - pause_.*

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

HBase RegionServer Compaction Queue Monitoring Thresholds

Description

The health test thresholds of the weighted average size of the HBase RegionServer compaction queue over a recent period. See HBase RegionServer Compaction Queue Monitoring Period.

Related Name

Default Value

Warning: 10.0, Critical: Never

API Name

regionserver_compaction_queue_thresholds

Required

false

HBase RegionServer Compaction Queue Monitoring Period

Description

The period over which to compute the moving average of the compaction queue size.

Related Name

Default Value

5 minute(s)

API Name

regionserver_compaction_queue_window

Required

false

HBase Region Server Connectivity Tolerance at Startup

Description

The amount of time to wait for the HBase Region Server to fully start up and connect to the HBase Master before enforcing the connectivity check.

Related Name

Default Value

3 minute(s)

API Name

regionserver_connectivity_tolerance

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

regionserver_fd_thresholds

Required

false

HBase RegionServer Flush Queue Monitoring Thresholds

Description

The health test thresholds of the average size of the HBase RegionServer flush queue over a recent period. See HBase RegionServer Flush Queue Monitoring Period.

Related Name

Default Value

Warning: 10.0, Critical: Never

API Name

regionserver_flush_queue_thresholds

Required

false

HBase RegionServer Flush Queue Monitoring Period

Description

The period over which to compute the moving average of the flush queue size.

Related Name

Default Value

5 minute(s)

API Name

regionserver_flush_queue_window

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

regionserver_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

regionserver_gc_duration_window

Required

false

RegionServer Host Health Test

Description

When computing the overall RegionServer health, consider the host's health.

Related Name

Default Value

true

API Name

regionserver_host_health_enabled

Required

false

HBase RegionServer to Master Connectivity Test

Description

Enables the health test that the RegionServer is connected to the Master

Related Name

Default Value

true

API Name

regionserver_master_connectivity_enabled

Required

false

HBase RegionServer Memstore Size Thresholds

Description

The health test thresholds of the total size of RegionServer's memstores. Specified as a percentage of the configured upper limit. See Maximum Size of All Memstores in RegionServer.

Related Name

Default Value

Warning: 95.0 %, Critical: 100.0 %

API Name

regionserver_memstore_size_thresholds

Required

false

HBase RegionServer HDFS Read Latency Thresholds

Description

The health test thresholds of the latency that the RegionServer sees for HDFS read operations

Related Name

Default Value

Warning: 50 millisecond(s), Critical: 100 millisecond(s)

API Name

regionserver_read_latency_thresholds

Required

false

HBase RegionServer HDFS Read Latency Monitoring Period

Description

The period over which to compute the moving average of the HDFS read latency of the HBase RegionServer.

Related Name

Default Value

5 minute(s)

API Name

regionserver_read_latency_window

Required

false

RegionServer Process Health Test

Description

Enables the health test that the RegionServer's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

regionserver_scm_health_enabled

Required

false

Percentage of Heap Used by HStoreFile Index

Description

The health test thresholds of the size used by the HStoreFile index. Specified as a percentage of the total heap size.

Related Name

Default Value

Warning: 10.0 %, Critical: Never

API Name

regionserver_store_file_idx_size_thresholds

Required

false

HBase RegionServer HDFS Sync Latency Thresholds

Description

The health test thresholds for the latency of HDFS write operations that the RegionServer detects

Related Name

Default Value

Warning: 500 millisecond(s), Critical: 5 second(s)

API Name

regionserver_sync_latency_thresholds

Required

false

HBase RegionServer HDFS Sync Latency Monitoring Period

Description

The period over which to compute the moving average of the HDFS sync latency of the HBase RegionServer.

Related Name

Default Value

5 minute(s)

API Name

regionserver_sync_latency_window

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

regionserver_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

regionserver_web_metric_collection_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.

- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HBase Hash Type

Description

The hashing algorithm for use in HashFunction. Two values are supported: 'murmur' (for MurmurHash) and 'jenkins' (for JenkinsHash).

Related Name

hbase.hash.type

Default Value

murmur

API Name

hbase_hash_type

Required

false

HBase HRegion Major Compaction

Description

The time, in milliseconds, between 'major' compactions of all HStoreFiles in a region. To disable automated major compactions, set this value to 0.

Related Name

hbase.hregion.majorcompaction

Default Value

7 day(s)

API Name

hbase_hregion_majorcompaction

Required

false

HBase HRegion Major Compaction Jitter

Description

Jitter outer bound for major compactions.
On each RegionServer, the hbase.region.majorcompaction
interval is multiplied by a random fraction that is inside the bounds of this
maximum. This + or - product is added to when the next
major compaction is to run. Major compaction
should not occur on every RegionServer at the same time. The
smaller this number, the closer together the compactions.

Related Name

hbase.hregion.majorcompaction.jitter

Default Value

0.5

API Name

hbase_hregion_majorcompaction_jitter

Required

false

HBase Maximum File Size

Description

Maximum HStoreFile size. If any one of a column families' HStoreFiles has grown to exceed this value, the hosting HRegion is split in two.

Related Name

hbase.hregion.max.filesize

Default Value

10 GiB

API Name

hbase_hregion_max_filesize

Required

false

HBase Memstore Block Multiplier

Description

Blocks writes if the size of the memstore increases to the value of 'hbase.hregion.block.memstore' multiplied by the value of 'hbase.hregion.flush.size' bytes. This setting is useful for preventing runaway memstore during spikes in update traffic. Without an upper-bound, memstore fills such that when it flushes, the resultant process of flushing files take a long time to compact or split, or worse, an "out of memory" error occurs.

Related Name

hbase.hregion.memstore.block.multiplier

Default Value

2

API Name

hbase_hregion_memstore_block_multiplier

Required

false

HBase Memstore Flush Size

Description

Memstore will be flushed to disk if size of the memstore exceeds this value in number of bytes. This value is checked by a thread that runs the frequency specified by hbase.server.thread.wakefrequency.

Related Name

hbase.hregion.memstore.flush.size

Default Value

128 MiB

API Name

hbase_hregion_memstore_flush_size

Required

false

Chunk Size Allocated by MSLAB Allocation Scheme

Description

The size of the chunks allocated by MSLAB, in bytes.

Related Name

hbase.hregion.memstore.mslab.chunksize

Default Value

2 MiB

API Name

hbase_hregion_memstore_mslab_chunksize

Required

false

Enable MSLAB Allocation Scheme

Description

Enable MemStore-Local Allocation Buffer (MSLAB) Allocation Scheme. Note: This feature is experimental in CDH3.

Related Name

hbase.hregion.memstore.mslab.enabled

Default Value

true

API Name

hbase_hregion_memstore_mslab_enabled

Required

false

Maximum Byte Array from MSLAB Allocation Scheme

Description

The maximum size byte array that should come from the MSLAB, in bytes.

Related Name

hbase.hregion.memstore.mslab.max.allocation

Default Value

256 KiB

API Name

hbase_hregion_memstore_mslab_max_allocation

Required

false

HBase Memstore Pre-close Flush Size

Description

If the memstores in a region are this size or larger when closing, run a pre-flush process to clear out memstores before putting up the region closed flag and taking the region offline. On close, a flush process is run under the close flag up to empty memory. During this time, the region is offline and no writes are taken. If the memstore content is large, the flush process could take a long time to complete. The pre-flush process cleans out the bulk of the memstore before putting up the close flag and taking the region offline, so that the flush process that runs under the close flag has little to do.

Related Name

hbase.hregion.preclose.flush.size

Default Value

5 MiB

API Name

hbase_hregion_preclose_flush_size

Required

false

HStore Blocking Store Files

Description

If there are more than this number of HStoreFiles in any one HStore, then updates are blocked for this HRegion until a compaction is completed, or until the value specified for 'hbase.hstore.blockingWaitTime' has been exceeded.

Related Name

hbase.hstore.blockingStoreFiles

Default Value

16

API Name

hbase_hstore_blockingStoreFiles

Required

false

HStore Blocking Wait Time

Description

The period of time that an HRegion will block updates after reaching the HStoreFile limit that is specified by 'hbase.hstore.blockingStoreFiles'. After this time has elapsed, the HRegion will stop blocking updates even if a compaction has not been completed.

Related Name

hbase.hstore.blockingWaitTime

Default Value

1 minute(s), 30 second(s)

API Name

hbase_hstore_blockingWaitTime

Required

false

Maximum Number of HStoreFiles Compaction

Description

Maximum number of HStoreFiles to compact per minor compaction.

Related Name

hbase.hstore.compaction.max

Default Value

API Name

hbase_hstore_compaction_max

Required

false

HStore Compaction Threshold

Description

If this number of HStoreFiles in any one HStore is exceeded, then a compaction is run to rewrite all HStoreFiles files as one HStoreFile. (One HStoreFile is written per flush of memstore.) You can delay compaction by specifying a larger number, but the compaction will take longer when it does run. During a compaction, updates cannot be flushed to disk. Long compactions require memory sufficient to carry the logging of all updates across the duration of the compaction. If too large, clients timeout during compaction.

Related Name

hbase.hstore.compactionThreshold

Default Value

3

API Name

hbase_hstore_compactionThreshold

Required

false

Enable Replication To Secondary Region Replicas

Description

Whether asynchronous WAL replication to the secondary region replicas is enabled.
If enabled, a replication peer named 'region_replica_replication' is created
that tails the logs and replicates the mutations to region replicas for tables that
have region replication > 1. Disabling this replication also
requires disabling the replication peer using shell or the ReplicationAdmin Java class.
Replication to secondary region replicas works over standard intercluster replication. If disabled explicitly, enable replication by setting 'hbase.replication' to true for this feature to work.

Related Name

hbase.region.replica.replication.enabled

Default Value

false

API Name

hbase_region_replica_replication_enabled

Required

false

HBase RegionServer Interface Class

Description

An interface that is assignable to HRegionInterface. Used in HBase Client for opening a proxy to a remote HBase RegionServer.

Related Name

hbase.regionserver.class

Default Value

API Name

hbase_regionserver_class

Required

false

RegionServer Codecs

Description

Comma-separated list of codecs that the RegionServer requires to start. Use this setting to make sure that all RegionServers joining a cluster are installed with a particular set of codecs.

Related Name

hbase.regionserver.codecs

Default Value

API Name

hbase_regionserver_codecs

Required

false

Low Watermark for Memstore Flush

Description

Controls when memstores are forced to flush to make room in memory. The memstore will begin flushing when this threshold is reached. Prior to CDH 5.8.0, this amount is the percentage of the heap size of the Region Server and you can set it equal to 'Maximum Size of All Memstores in RegionServer' for minimal possible flushing. In CDH 5.8.0 and later, this amount is the percentage of memstore memory and you can set it equal to 1.0 for minimal possible flushing.

Related Name

hbase.regionserver.global.memstore.size.lower.limit

Default Value

0.95

API Name

hbase_regionserver_global_memstore_lowerLimit

Required

false

Maximum Size of All Memstores in RegionServer

Description

Maximum size of all memstores in a RegionServer before new updates are blocked and flushes are forced.

Related Name

hbase.regionserver.global.memstore.size

Default Value

0.4

API Name

hbase_regionserver_global_memstore_upperLimit

Required

false

HBase RegionServer Handler Count

Description

Number of RPC Server instances spun up on RegionServers.

Related Name

hbase.regionserver.handler.count

Default Value

30

API Name

hbase_regionserver_handler_count

Required

false

HLog Reader Implementation

Description

The HLog file reader implementation.

Related Name

hbase.regionserver.hlog.reader.impl

Default Value

API Name

hbase_regionserver_hlog_reader_impl

Required

false

HLog Writer Implementation

Description

The HLog file writer implementation.

Related Name

hbase.regionserver.hlog.writer.impl

Default Value

API Name

hbase_regionserver_hlog_writer_impl

Required

false

HBase RegionServer Lease Period

Description

The lease period, in milliseconds, for the HBase RegionServer. Clients must report in within this period or else they are considered dead.

Related Name

hbase.client.scanner.timeout.period

Default Value

1 minute(s)

API Name

hbase_regionserver_lease_period

Required

false

HBase RegionServer Log Roll Period

Description

Period, in milliseconds, at which to roll the commit log.

Related Name

hbase.regionserver.logroll.period

Default Value

1 hour(s)

API Name

hbase_regionserver_logroll_period

Required

false

Maximum number of Write-Ahead Log (WAL) files

Description

Maximum number of Write-Ahead Log (WAL) files. This value multiplied by HDFS Block Size (dfs.blocksize) is the size of the WAL that will need to be replayed when a server crashes. This value is inversely proportional to the frequency of flushes to disk.

Related Name

hbase.regionserver.maxlogs

Default Value

32

API Name

hbase_regionserver_maxlogs

Required

false

HBase RegionServer Meta-Handler Count

Description

Number of handlers for processing priority requests in a RegionServer.

Related Name

hbase.regionserver.metahandler.count

Default Value

10

API Name

hbase_regionserver_metahandler_count

Required

false

HBase RegionServer Message Interval

Description

Interval, in milliseconds, between messages from the RegionServer to the HBase Master. Use a high value such as 3000 for clusters that have more than 10 hosts.

Related Name

hbase.regionserver.msginterval

Default Value

3 second(s)

API Name

hbase_regionserver_msginterval

Required

false

RegionServer Reservation Blocks

Description

The number of reservation blocks that are used to prevent unstable RegionServers caused by an OOME.

Related Name

hbase.regionserver.nbreservationblocks

Default Value

4

API Name

hbase_regionserver_nbreservationblocks

Required

false

Synch Interval of HLog Entries

Description

Sync the HLog to HDFS after this interval, in milliseconds, if it has not accumulated the number of HLog Entries specified to trigger a sync.

Related Name

hbase.regionserver.optionallogflushinterval

Default Value

1 second(s)

API Name

hbase_regionserver_optionallogflushinterval

Required

false

WAL Delegate Provider

Description

The write ahead log (WAL) delegate provider.

Related Name

hbase.wal.regiongrouping.delegate.provider

Default Value

filesystem

API Name

hbase_regionserver_regiongrouping_delegate_provider

Required

false

HBase Region Split Limit

Description

Limit for the number of regions after which no more region splitting should take place. This is not a hard limit for the number of regions but acts as a guideline for the RegionServer to stop splitting after a certain limit.

Related Name

hbase.regionserver.regionSplitLimit

Default Value

2147483647

API Name

hbase_regionserver_regionSplitLimit

Required

false

Per-RegionServer Number of WAL Pipelines

Description

When using Multiple HDFS WAL as the WALProvider, sets how many write-ahead-logs each RegionServer should run. Will result in this number of HDFS pipelines. Writes for a given Region only go to a single pipeline, spreading total RegionServer load.

Related Name

hbase.wal.regiongrouping.numgroups

Default Value

1

API Name

hbase_regionserver_wal_pipelines

Required

false

WAL Provider

Description

The implementation that should be used by the RegionServer for the write-ahead-log. The HBase Default (HBase Internal HDFS Client) - is deprecated since it is redundant with Single HDFS WAL.

Related Name

hbase.wal.provider

Default Value

multiwal

API Name

hbase_regionserver_wal_provider

Required

false

WAL HSM Storage Policy

Description

The Hierarchical Storage Management policy that should be used by the RegionServer for the write-ahead-log. Using an SSD policy will have no effect unless HDFS HSM is configured to know which drives are SSDs. See Enabling HSM with HBase .

Related Name

hbase.wal.storage.policy

Default Value

NONE

API Name

hbase_regionserver_wal_storage_policy

Required

false

HFile Block Cache Size

Description

Percentage of maximum heap (-Xmx setting) to allocate to block cache used by HFile/StoreFile. To disable, set this value to 0 .

Related Name

hfile.block.cache.size

Default Value

0.4

API Name

hfile_block_cache_size

Required

false

Performance

RegionServer IPC Read Threadpool Size

Description

Read threadpool size used by the RegionServer HBase IPC Server.

Related Name

hbase.ipc.server.read.threadpool.size

Default Value

10

API Name

hbase_ipc_server_read_threadpool_size

Required

false

Region Mover Threads

Description

Number of threads to use while loading and unloading regions to or from a RegionServer. Can be used to increase the speed of decommissioning or rolling restart operations.

Related Name

Default Value

1

API Name

hbase_regionserver_regionmover_thread_count

Required

true

RegionServer Small Compactions Thread Count

Description

Number of threads for completing small compactions.

Related Name

hbase.regionserver.thread.compaction.small

Default Value

1

API Name

hbase_regionserver_thread_compaction_small

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

32768

API Name

rlimit_fds

Required

false

Ports and Addresses

HBase RegionServer Bind to Wildcard Address

Description

When true, HBase RegionServer will bind to 0.0.0.0. Only available in CDH 4.3 and later.

Related Name

hbase.regionserver.ipc.address

Default Value

true

API Name

hbase_regionserver_bind_to_wildcard_address

Required

true

RegionServer DNS Network Interface

Description

The name of the DNS Network Interface from which a RegionServer should report its IP address.

Related Name

hbase.regionserver.dns.interface

Default Value

API Name

hbase_regionserver_dns_interface

Required

false

RegionServer DNS Nameserver

Description

The host name or IP address of the DNS name server which a RegionServer should use to determine the host name used by the HBase Master for communication and display purposes.

Related Name

hbase.regionserver.dns.nameserver

Default Value

API Name

hbase_regionserver_dns_nameserver

Required

false

HBase RegionServer Web UI Address

Description

The address for the HBase RegionServer web UI

Related Name

hbase.regionserver.info.bindAddress

Default Value

API Name

hbase_regionserver_info_bindAddress

Required

false

HBase RegionServer Web UI port

Description

The port for the HBase RegionServer web UI. Set to -1 to disable RegionServer web UI.

Related Name

hbase.regionserver.info.port

Default Value

16030

API Name

hbase_regionserver_info_port

Required

false

HBase RegionServer Port

Description

The port that an HBase RegionServer binds to.

Related Name

hbase.regionserver.port

Default Value

16020

API Name

hbase_regionserver_port

Required

false

Resource Management

Java Heap Size of HBase RegionServer in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

hbase_regionserver_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Require EXEC privilege to execute coprocessor calls

Description

If this setting is enabled and ACL based access control is active (the AccessController coprocessor is installed either as a system coprocessor or on a table as a table coprocessor) then you must grant all relevant users EXEC privilege if they require the ability to execute coprocessor endpoint calls. EXEC privilege, like any other permission, can be granted globally to a user, or to a user on a per table or per namespace basis. For more information on coprocessor endpoints, see the coprocessor section of the HBase online manual. For more information on granting or revoking permissions using the AccessController, see the security section of the HBase online manual.

Related Name

hbase.security.exec.permission.checks

Default Value

false

API Name

hbase_security_exec_permission_checks

Required

false

HBase Region Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HBase Region Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

regionserver_truststore_file

Required

false

HBase Region Server TLS/SSL Trust Store Password

Description

The password for the HBase Region Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

regionserver_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: BucketCache IOEngine

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the BucketCache IOEngine parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_bucketcache_ioengine

Required

true

Suppress Parameter Validation: HBase Coprocessor Region Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Coprocessor Region Classes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_coprocessor_region_classes

Required

true

Suppress Parameter Validation: HBase HRegion Major Compaction

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase HRegion Major Compaction parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_hregion_majorcompaction

Required

true

Suppress Parameter Validation: Netty native library working directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Netty native library working directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_netty_native_workdir

Required

true

Suppress Parameter Validation: HBase RegionServer Interface Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase RegionServer Interface Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_class

Required

true

Suppress Parameter Validation: RegionServer Codecs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer Codecs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_codecs

Required

true

Suppress Parameter Validation: RegionServer Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_config_safety_valve

Required

true

Suppress Parameter Validation: RegionServer DNS Network Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer DNS Network Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_dns_interface

Required

true

Suppress Parameter Validation: RegionServer DNS Nameserver

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer DNS Nameserver parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_dns_nameserver

Required

true

Suppress Configuration Validator: HBase Region Server Memstore Lower Limit Validator

Description

Whether to suppress configuration warnings produced by the HBase Region Server Memstore Lower Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_global_memstore_lowerlimit_validator

Required

true

Suppress Parameter Validation: HLog Reader Implementation

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HLog Reader Implementation parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_hlog_reader_impl

Required

true

Suppress Parameter Validation: HLog Writer Implementation

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HLog Writer Implementation parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_hlog_writer_impl

Required

true

Suppress Parameter Validation: HBase RegionServer Web UI Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase RegionServer Web UI Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_info_bindaddress

Required

true

Suppress Parameter Validation: HBase RegionServer Web UI port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase RegionServer Web UI port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_info_port

Required

true

Suppress Parameter Validation: Java Heap Size of HBase RegionServer in Bytes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of HBase RegionServer in Bytes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_java_heapsize

Required

true

Suppress Parameter Validation: Java Configuration Options for HBase RegionServer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HBase RegionServer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_java_opts

Required

true

Suppress Parameter Validation: RegionServer Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_log_dir

Required

true

Suppress Configuration Validator: HBase RegionServer Multiple HDFS WAL with Replication Validator

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Multiple HDFS WAL with Replication Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_multiwal_replication_validator

Required

true

Suppress Parameter Validation: HBase RegionServer Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase RegionServer Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_port

Required

true

Suppress Parameter Validation: Write-Ahead Log (WAL) Codec Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Write-Ahead Log (WAL) Codec Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_wal_codec

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: RegionServer Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: RegionServer File Descriptor Limit Validator

Description

Whether to suppress configuration warnings produced by the RegionServer File Descriptor Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_fd_limit_validator

Required

true

Suppress Parameter Validation: RegionServer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RegionServer Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: HBase Region Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Region Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_truststore_file

Required

true

Suppress Parameter Validation: HBase Region Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Region Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_truststore_password

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_audit_health

Required

true

Suppress Health Test: Compaction Queue Size

Description

Whether to suppress the results of the Compaction Queue Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_compaction_queue

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_file_descriptor

Required

true

Suppress Health Test: Flush Queue Size

Description

Whether to suppress the results of the Flush Queue Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_flush_queue

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_log_directory_free_space

Required

true

Suppress Health Test: Cluster Connectivity

Description

Whether to suppress the results of the Cluster Connectivity heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_master_connectivity

Required

true

Suppress Health Test: Memstore Size

Description

Whether to suppress the results of the Memstore Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_memstore_size

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_otelcol_health

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_scm_health

Required

true

Suppress Health Test: Store File Index Size

Description

Whether to suppress the results of the Store File Index Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_store_file_idx_size

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_region_server_web_metric_collection

Required

true

Service-Wide

Advanced

HBase Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

For advanced use only, a string to be inserted into atlas-application.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

application_properties_safety_valve

Required

false

Enable Atlas Hook

Description

Enable Atlas Hook to generate Metadata / Lineage information. This Atlas hook is only for the instance of HBase that the Atlas service is using. No other instance of HBase can or should enable this hook.

Related Name

Default Value

false

API Name

hbase_atlas_hook_enable

Required

false

HBase Coprocessor Abort on Error

Description

Set to true to cause the hosting server (Master or RegionServer) to abort if a coprocessor throws a Throwable object that is not IOException or a subclass of IOException. Setting it to true might be useful in development environments where one wants to terminate the server as soon as possible to simplify coprocessor failure analysis.

Related Name

hbase.coprocessor.abortonerror

Default Value

false

API Name

hbase_coprocessor_abort_on_error

Required

false

HBase Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hbase_core_site_safety_valve

Required

false

Dynamic Jars Directory

Description

The directory from which the custom filter, comparator, and exception JARs can be loaded without the need to restart. However, an already loaded class would not be un-loaded. Specify a full hadoop filesystem URL.

Related Name

hbase.dynamic.jars.dir

Default Value

API Name

hbase_dynamic_jars_dir

Required

false

Enable HBase Canary

Description

Start a process to periodically check that RegionServer is alive when RegionServer is started. Note: This canary is different from the Cloudera Service Monitoring canary and is provided by the HBase service itself.

Related Name

Default Value

false

API Name

hbase_regionserver_enable_canary

Required

false

HBase replication auxiliary info

Description

Do not modify this value!

Related Name

Default Value

API Name

hbase_replication_auxiliary_info

Required

false

HBase replication setup status

Description

Do not modify this value!

Related Name

Default Value

API Name

hbase_replication_setup_statuses

Required

false

HBase Service Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

For advanced use only, a string to be inserted into hbase-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hbase_service_config_safety_valve

Required

false

HBase Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hbase_service_env_safety_valve

Required

false

Skip Region Reload During Rolling Restart

Description

Whether the step to reload regions back onto the original RegionServers should be skipped during rolling restart. This can be used to increase the speed of rolling restart or upgrade operations, but can result in regions being moved multiple times, decreasing performance for clients during rolling restart.

Related Name

Default Value

false

API Name

hbase_skip_reload_during_rr

Required

true

HBase Snapshot Service Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only, a string to be inserted into mapred-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hbase_snapshot_mapreduce_config_safety_valve

Required

false

HBase Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

For advanced use only, a string to be inserted into ssl-server.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hbase_ssl_server_safety_valve

Required

false

Enable dynamic loading of filter, comparator and exception classes

Description

Whether to dynamically load certain classes

Related Name

hbase.use.dynamic.jars

Default Value

false

API Name

hbase_use_dynamic_jars

Required

true

HBase User to Impersonate

Description

The user the management services impersonate when connecting to HBase. If no value is specified, the HBase superuser is used.

Related Name

Default Value

API Name

hbase_user_to_impersonate

Required

false

HBASE Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hbase

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hbase

API Name

process_username

Required

true

HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-audit.xml

Description

For advanced use only, a string to be inserted into ranger-hbase-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-hbase-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-security.xml

Description

For advanced use only, a string to be inserted into ranger-hbase-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Backup

Enable Indexing

Description

Allow indexing of tables in HBase by Lily HBase Indexer. Note: Replication must be enabled for indexing to work.

Related Name

Default Value

false

API Name

hbase_enable_indexing

Required

false

Enable Replication

Description

Allow HBase tables to be replicated.

Related Name

hbase.replication

Default Value

false

API Name

hbase_enable_replication

Required

false

Replication Batch Size

Description

Maximum number of hlog entries to replicate in one go. If this is large, and a consumer takes a while to process the events, the HBase RPC call will time out.

Related Name

replication.source.nb.capacity

Default Value

1000

API Name

hbase_replication_source_nb_capacity

Required

false

Replication Source Ratio

Description

Ratio of Lily HBase Indexers used by each HBase RegionServer while doing replication.

Related Name

replication.source.ratio

Default Value

1.0

API Name

hbase_replication_source_ratio

Required

false

Enable Snapshots

Description

Enable snapshots. Disabling snapshots requires deletion of all snapshots before restarting the HBase master; the HBase master will not start if snapshots are disabled and snapshots exist.

Related Name

hbase.snapshot.enabled

Default Value

true

API Name

hbase_snapshot_enabled

Required

false

HBase Master Snapshot Timeout

Description

The maximum amount of time the HBase master waits for a snapshot to complete.

Related Name

hbase.snapshot.master.timeout.millis

Default Value

5 minute(s)

API Name

hbase_snapshot_master_timeout_millis

Required

false

HBase RegionServer Snapshot Timeout

Description

The maximum amount of time the Hbase RegionServer waits for a snapshot to complete.

Related Name

hbase.snapshot.region.timeout

Default Value

5 minute(s)

API Name

hbase_snapshot_region_timeout

Required

false

AWS S3 Access Key ID for Remote Snapshots

Description

Access key ID required to access AWS S3 to store remote snapshots.

Related Name

Default Value

API Name

hbase_snapshot_s3_access_key_id

Required

false

AWS S3 Path for Remote Snapshots

Description

AWS S3 path where remote snapshots should be stored.

Related Name

Default Value

API Name

hbase_snapshot_s3_path

Required

false

Scheduler Pool for Remote Snapshots in AWS S3

Description

Name of the scheduler pool to use for MR jobs created during export/import of remote snapshots in AWS S3.

Related Name

Default Value

API Name

hbase_snapshot_s3_scheduler_pool

Required

false

AWS S3 Secret Access Key for Remote Snapshots

Description

AWS secret access key required to access S3 to store remote snapshots.

Related Name

Default Value

API Name

hbase_snapshot_s3_secret_access_key

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for HBase events:

- allowed: whether the operation was allowed or denied.
- username: the user performing the action.
- tableName: the table affected by the operation.
- family: the column family affected by the operation.
- qualifier: the qualifier the operation.
- action: the action being performed.

The default HBase audit event filter discards events that affect the internal -ROOT-, .META. and _acl_ tables.

Related Name

navigator.event.filter

Default Value

comment: [The default HBase audit event filter discards events that affect the , internal -ROOT-, .META. and _acl_ tables.], defaultAction: accept, rules: [action: discard, fields: [name: tableName, match: (?:-ROOT-|.META.|_acl_|hbase:meta|hbase:acl)]]

API Name

navigator_audit_event_filter

Required

false

Audit Queue Policy

Description

Action to take when the audit event queue is full. Drop the event or shutdown the affected process.

Related Name

navigator.batch.queue_policy

Default Value

DROP

API Name

navigator_audit_queue_policy

Required

false

Audit Event Tracker

Description

Configures the rules for event tracking and coalescing. This feature is used to define equivalency between different audit events. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the "tracked" events according to the rules defined here. Event trackers are defined in a JSON object like the following: { "timeToLive" : [integer], "fields" : [{ "type" : [string], "name" : [string] }] } Where:

- timeToLive: maximum amount of time an event will be tracked, in milliseconds. Must be provided. This defines how long, since it's first seen, an event will be tracked. A value of 0 disables tracking.
- fields: list of fields to compare when matching events against tracked events.

Each field has an evaluator type associated with it. The evaluator defines how the field data is to be compared. The following evaluators are available:

- value: uses the field value for comparison.
- username: treats the field value as a user name, and ignores any host-specific data. This is useful for environment using Kerberos, so that only the principal name and realm are compared.

The following is the list of fields that can used to compare HBase events:

- operation: the HBase operation being performed.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- tableName: the name of the table affected by the operation.
- family: the column family affected by the operation.
- qualifier: the qualifier of the operation.

The default event tracker for HBase services defines equality by comparing the username, operation, table name, family, and qualifier of the events.

Related Name

navigator_event_tracker

Default Value

comment: [The default event tracker for HBase services defines equality by , comparing the username, operation, table name, family, and qualifier of , the events.], timeToLive: 60000, fields: [type: value, name: tableName , type: value, name: family , type: value, name: qualifier , type: value, name: operation , type: username, name: username]

API Name

navigator_event_tracker

Required

false

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/hbase/audit

API Name

audit_event_log_dir

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Number of Audit Logs to Retain

Description

Maximum number of rolled-over audit logs to retain. The logs are not deleted if they contain audit events that have not yet been propagated to the Audit Server.

Related Name

navigator.client.max_num_audit_log

Default Value

10

API Name

navigator_client_max_num_audit_log

Required

false

Monitoring

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

HBase Active Master Detection Window

Description

The tolerance window that will be used in HBase service tests that depend on detection of the active HBase Master.

Related Name

Default Value

3 minute(s)

API Name

hbase_active_master_detection_window

Required

false

Backup Masters Health Test

Description

When computing the overall HBase cluster health, consider the health of the backup HBase Masters.

Related Name

Default Value

true

API Name

hbase_backup_masters_health_enabled

Required

false

HBase Canary Unhealthy Region Count Alert Threshold

Description

An alert is published if the HBase region health canary detects at least this many unhealthy regions. This setting takes precedence over the hbase_canary_alert_unhealthy_region_percent_threshold config.

Related Name

Default Value

API Name

hbase_canary_alert_unhealthy_region_count_threshold

Required

false

HBase Canary Unhealthy Region Percentage Alert Threshold

Description

An alert is published if the HBase region health canary detects at least this percentage of total regions are unhealthy. This threshold is used if the explicit count is not set via the hbase_canary_alert_unhealthy_region_count_threshold config.

Related Name

Default Value

0.1

API Name

hbase_canary_alert_unhealthy_region_percent_threshold

Required

false

HBase Erasure Code Canary

Description

Enables the canary that checks if erasure coding is set for hbase root directory.

Related Name

Default Value

true

API Name

hbase_erasure_code_canary_enabled

Required

false

Active Master Health Test

Description

When computing the overall HBase cluster health, consider the active HBase Master's health.

Related Name

Default Value

true

API Name

hbase_master_health_enabled

Required

false

HBase Region Health Canary

Description

Enables the canary that checks HBase region availability by scanning a row from every region.

Related Name

Default Value

true

API Name

hbase_region_health_canary_enabled

Required

false

HBase Region Health Canary Exclude Tables

Description

Tables to exclude in the HBase Region Health Canary which will scan a row from every region.

Related Name

Default Value

API Name

hbase_region_health_canary_exclude_tables

Required

false

HBase Region Health Canary Slow Run Alert Enabled

Description

An alert is published if the HBase region health canary runs slowly.

Related Name

Default Value

true

API Name

hbase_region_health_canary_slow_run_alert_enabled

Required

false

Healthy RegionServer Monitoring Thresholds

Description

The health test thresholds of the overall RegionServer health. The check returns "Concerning" health if the percentage of "Healthy" RegionServers falls below the warning threshold. The check

is unhealthy if the total percentage of "Healthy" and "Concerning" RegionServers falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

hbase_regionservers_healthy_thresholds

Required

false

Log Event Retry Frequency

Description

The frequency in which the log4j event publication appender will retry sending undelivered log events to the Event server, in seconds

Related Name

Default Value

30

API Name

log_event_retry_frequency

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>zookeeper.recovery.retry</name> <value>0</value> </property> <property> <name>zookeeper.recovery.retry.intervalmill</name> <value>3000</value> </property> <property> <name>hbase.zookeeper.recoverable.waittime</name> <value>1000</value> </property> <property> <name>zookeeper.session.timeout</name> <value>30000</value> </property> <property> <name>hbase.rpc.timeout</name> <value>10000</value> </property> <property> <name>hbase.client.retries.number</name> <value>1</value> </property> <property> <name>hbase.client.rpc.maxattempts</name> <value>1</value> </property> <property> <name>hbase.client.operation.timeout</name> <value>10000</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Atlas Service

Description

Name of the Atlas service that this Hbase service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Generate HADOOP_CREDSTORE_PASSWORD

Description

Flag to enable or disable the generation of HADOOP_CREDSTORE_PASSWORD.

Related Name

generate_jceks_password

Default Value

true

API Name

generate_jceks_password

Required

false

Maximum Size of HBase Client KeyValue

Description

Specifies the combined maximum allowed size of a KeyValue instance. This option configures an upper boundary for a single entry saved in a storage file. This option prevents a region from splitting if the data is too large. Set this option to a fraction of the maximum region size. To disable this check, use a value of zero or less.

Related Name

hbase.client.keyvalue.maxsize

Default Value

10 MiB

API Name

hbase_client_keyvalue_maxsize

Required

false

HBase Client Pause

Description

A general client pause time value. Used mostly as a time period to wait before retrying operations such as a failed get or region lookup.

Related Name

hbase.client.pause

Default Value

100 millisecond(s)

API Name

hbase_client_pause

Required

false

Maximum HBase Client Retries

Description

Maximum number of client retries. Used as a maximum for all operations such as fetching of the root region from the root RegionServer, getting a cell's value, and starting a row update.

Related Name

hbase.client.retries.number

Default Value

10

API Name

hbase_client_retries_number

Required

false

HBase Client Scanner Caching

Description

Number of rows to fetch when calling next on a scanner if it is not served from memory. Higher caching values enable faster scanners but require more memory and some calls of next may take longer when the cache is empty.

Related Name

hbase.client.scanner.caching

Default Value

100

API Name

hbase_client_scanner_caching

Required

false

HBase Client Write Buffer

Description

Write buffer size in bytes. A larger buffer requires more memory on both the client and the server because the server instantiates the passed write buffer to process it but reduces the number of remote procedure calls (RPC). To estimate the amount of server memory used, multiply the value of 'hbase.client.write.buffer' by the value of 'hbase.regionserver.handler.count'.

Related Name

hbase.client.write.buffer

Default Value

2 MiB

API Name

hbase_client_write_buffer

Required

false

Graceful Shutdown Timeout

Description

Timeout for graceful shutdown of this HBase service. Once this timeout is reached, any remaining running roles are abruptly shutdown. A value of 0 means no timeout.

Related Name

Default Value

3 minute(s)

API Name

hbase_graceful_stop_timeout

Required

true

HBoss Maximum Number of S3 Connections

Description

Controls the maximum number of simultaneous connections to S3 from HBoss.

Related Name

fs.s3a.connection.maximum

Default Value

300

API Name

hbase_hboss_fs_s3a_connection_maximum

Required

false

HBoss S3A Implementation Class

Description

The implementation to use (HBoss) for S3A FileSystem access.

Related Name

fs.s3a.impl

Default Value

org.apache.hadoop.hbase.oss.HBaseObjectStoreSemantics

API Name

hbase_hboss_fs_s3a_impl

Required

false

HBoss Maximum Number of Concurrent S3 Uploads

Description

Maximum number of concurrent active (part)uploads, which each use a thread from the threadpool.

Related Name

fs.s3a.threads.max

Default Value

200

API Name

hbase_hboss_fs_s3a_threads_max

Required

false

HBoss Lock Implementation

Description

The HBoss implementation to use for distributing locking on top of S3A.

Related Name

fs.hboss.sync.impl

Default Value

org.apache.hadoop.hbase.oss.sync.ZKTreeLockManager

API Name

hbase_hboss_fs_sync_impl

Required

false

HBoss Wrapped S3A Implementation Class

Description

The implementation which HBoss should instantiate for S3A FileSystem access.

Related Name

fs.hboss.fs.s3a.impl

Default Value

org.apache.hadoop.fs.s3a.S3AFileSystem

API Name

hbase_hboss_wrapped_fs_s3a_impl

Required

false

Enable HBase REST Server Proxy Users

Description

Use this to allow proxy users on HBase REST server, which is mainly needed for "doAs" functionality.

Related Name

hbase.rest.support.proxyuser

Default Value

true

API Name

hbase_restserver_support_proxyuser

Required

false

RPC Timeout

Description

Timeout for all HBase RPCs in milliseconds.

Related Name

hbase.rpc.timeout

Default Value

1 minute(s)

API Name

hbase_rpc_timeout

Required

false

HBase Server Thread Wake Frequency

Description

Period of time, in milliseconds, to pause between searches for work. Used as a sleep interval by service threads such as a META scanner and log roller.

Related Name

hbase.server.thread.wakefrequency

Default Value

10 second(s)

API Name

hbase_server_thread_wakefrequency

Required

false

HBase Superusers

Description

List of users or groups, who are allowed full privileges, regardless of stored ACLs, across the cluster. Only used when HBase security is enabled.

Related Name

hbase.superuser

Default Value

API Name

hbase_superuser

Required

false

Enable HBase Thrift Http Server

Description

Use this to enable Http server usage on thrift, which is mainly needed for "doAs" functionality.

Related Name

hbase.regionserver.thrift.http

Default Value

false

API Name

hbase_thriftserver_http

Required

false

Enable HBase Thrift Proxy Users

Description

Use this to allow proxy users on thrift gateway, which is mainly needed for "doAs" functionality.

Related Name

hbase.thrift.support.proxyuser

Default Value

false

API Name

hbase_thriftserver_support_proxyuser

Required

false

HDFS WAL Directory

Description

The HDFS directory used for the WAL, shared by HBase RegionServers.

Related Name

hbase.wal.dir

Default Value

API Name

hbase_wal_dir

Required

false

HDFS Root Directory

Description

The HDFS directory shared by HBase RegionServers.

Related Name

hbase.rootdir

Default Value

/hbase

API Name

hdfs_rootdir

Required

true

HDFS Service

Description

Name of the HDFS service that this HBase service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Ranger Service Name

Description

Name of the Ranger service/repository where service related data will be stored

Related Name

ranger.plugin.hbase.service.name

Default Value

GENERATED_RANGER_SERVICE_NAME

API Name

ranger_plugin_service_name

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hbase.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hbase.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Hbase service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

ZooKeeper Connection Retry Pause Duration

Description

Period of time, in milliseconds, to pause between connection retries to ZooKeeper. Used together with ${zookeeper.retries} in an exponential backoff fashion when making queries to ZooKeeper.

Related Name

zookeeper.pause

Default Value

API Name

zookeeper_pause

Required

false

ZooKeeper Connection Retries

Description

The number of times to retry connections to ZooKeeper. Used for reading and writing root region location. Used together with ${zookeeper.pause} in an exponential backoff fashion when making queries to ZooKeeper.

Related Name

zookeeper.retries

Default Value

API Name

zookeeper_retries

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this HBase service instance depends on.

Related Name

Default Value

API Name

zookeeper_service

Required

true

ZooKeeper Session Timeout

Description

ZooKeeper session timeout in milliseconds. HBase passes this to the ZooKeeper quorum as the suggested maximum time for a session. See http://hadoop.apache.org/zookeeper/docs/current/zookeeperProgrammers.html#ch_zkSessions The client sends a requested timeout, the server responds with the timeout that it can give the client.

Related Name

zookeeper.session.timeout

Default Value

60000

API Name

zookeeper_session_timeout

Required

false

ZooKeeper Znode Parent

Description

The root znode for HBase in ZooKeeper. All of HBase's ZooKeeper files that are configured with a relative path will go under this node. By default, all of HBase's ZooKeeper file paths are configured with a relative path, so they will all go under this directory unless changed.

Related Name

zookeeper.znode.parent

Default Value

/hbase

API Name

zookeeper_znode_parent

Required

true

ZooKeeper Znode Rootserver

Description

Path to ZooKeeper Node holding root region location. This is written by the HBase Master and read by clients and RegionServers. If a relative path is given, the parent folder will be ${zookeeper.znode.parent}. By default, the root location is stored at /hbase/root-region-server.

Related Name

zookeeper.znode.rootserver

Default Value

root-region-server

API Name

zookeeper_znode_rootserver

Required

true

Performance

Enable HDFS Short-Circuit Read

Description

Enable HDFS short-circuit read. This allows a client colocated with the DataNode to read HDFS file blocks directly. This gives a performance boost to distributed clients that are aware of locality.

Related Name

dfs.client.read.shortcircuit

Default Value

true

API Name

dfs_client_read_shortcircuit

Required

false

HDFS Hedged Read Threadpool Size

Description

Size of the threadpool used for hedged reads in hdfs clients. If a read from a block is slow, a parallel 'hedged' read will be started against a different block replica. The first one to return with a result is used while the other one is cancelled. This 'hedged' read feature helps rein in the outliers. A value of zero disables the feature.

Related Name

dfs.client.hedged.read.threadpool.size

Default Value

0

API Name

hbase_server_dfs_client_hedged_read_threadpool_size

Required

false

HDFS Hedged Read Delay Threshold

Description

Duration to wait before starting up a 'hedged' read.

Related Name

dfs.client.hedged.read.threshold.millis

Default Value

500 millisecond(s)

API Name

hbase_server_dfs_client_hedged_read_threshold_millis

Required

false

SplitLog Manager Timeout

Description

Timeout (in ms) for the distributed log splitting manager to receive response from a worker.

Related Name

hbase.splitlog.manager.timeout

Default Value

2 minute(s)

API Name

hbase_service_splitlog_manager_timeout

Required

false

Proxy

HBase Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the HBase user to impersonate. The default '*' allows all groups. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_'. Note: This property is used only if HBase REST/Thrift Server Authentication is enabled.

Related Name

hadoop.proxyuser.hbase.groups

Default Value

*

API Name

hbase_proxy_user_groups_list

Required

false

HBase Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HBase user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that does not correspond to a host name, such as '_no_host'. Note: This property is used only if HBase REST/Thrift Server Authentication is enabled.

Related Name

hadoop.proxyuser.hbase.hosts

Default Value

*

API Name

hbase_proxy_user_hosts_list

Required

false

Security

Atlas Kafka Messages Spool Directory

Description

Spool directory for Atlas Kafka Messages.

Related Name

atlas.hook.spool.dir

Default Value

/var/log/hbase/atlas-spool

API Name

atlas_message_spool_path

Required

false

Enable Kerberos Authentication for HTTP Web-Consoles

Description

Enables Kerberos authentication for Hadoop HTTP web consoles for all roles of this service using the SPNEGO protocol. Note: This is effective only if Kerberos is enabled.

Related Name

Default Value

false

API Name

hadoop_secure_web_ui

Required

false

HBase Cell-Level ACLs

Description

Enable HBase cell-level ACLs.

Related Name

hbase.security.access.early_out

Default Value

false

API Name

hbase_cell_acl_authorization

Required

false

Web UI TLS/SSL Encryption Enabled

Description

Enable TLS/SSL encryption for HBase web UIs.

Related Name

hbase.ssl.enabled

Default Value

false

API Name

hbase_hadoop_ssl_enabled

Required

false

HBase REST Authentication

Description

If this is set to "kerberos", HBase REST Server will authenticate its clients. HBase Proxy User Hosts and Groups should be configured to allow specific users to access HBase through REST Server.

Related Name

hbase.rest.authentication.type

Default Value

simple

API Name

hbase_restserver_security_authentication

Required

false

HBase Row-Level Authorization

Description

Enable HBase row-level authorization.

Related Name

hbase.row.level.authorization

Default Value

false

API Name

hbase_row_level_authorization

Required

false

HBase Transport Security

Description

Configure the type of encrypted communication to be used with RPC.

Related Name

hbase.rpc.protection

Default Value

authentication

API Name

hbase_rpc_protection

Required

false

HBase Secure RPC Engine

Description

Set to true to use HBase Secure RPC Engine for remote procedure calls (RPC). This is only effective in simple authentication mode. Does not provide authentication for RPC calls, but provides user information in the audit logs. Changing this setting requires a restart of this and all dependent services and redeployment of client configurations, along with a restart of the Service Monitor management role.

Related Name

hbase.secure.rpc.engine

Default Value

false

API Name

hbase_secure_rpc_engine

Required

false

HBase Secure Authentication

Description

Choose the authentication mechanism used by HBase.

Related Name

hbase.security.authentication

Default Value

simple

API Name

hbase_security_authentication

Required

false

Assigned SPNEGO virtual groups

Description

Comma-separated list of Unix groups to define administrators of the HBase UI when SPNEGO authentication is enabled.

Related Name

hbase.security.authentication.spnego.admin.groups

Default Value

API Name

hbase_security_authentication_spnego_admin_groups

Required

false

HBase Secure Authorization

Description

Enable HBase authorization.

Related Name

hbase.security.authorization

Default Value

false

API Name

hbase_security_authorization

Required

false

HBase Thrift Authentication

Description

If this is set, HBase Thrift Server authenticates its clients. HBase Proxy User Hosts and Groups should be configured to allow specific users to access HBase through Thrift Server.

Related Name

hbase.thrift.security.qop

Default Value

none

API Name

hbase_thriftserver_security_authentication

Required

true

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hbase

API Name

kerberos_princ_name

Required

true

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hbase

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hbase/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hbase/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hbase.policy.cache.dir

Default Value

/var/lib/ranger/hbase/policy-cache

API Name

ranger_policy_cache_dir

Required

false

HBase TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when HBase is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

HBase TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HBase is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

HBase TLS/SSL Server Keystore File Password

Description

The password for the HBase keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

HBase ZooKeeper Secure Client Enabled

Description

Enable TLS connection to ZooKeeper in HBase client.

Related Name

hbase.zookeeper.property.client.secure

Default Value

false

API Name

zookeeper_secure_client_enabled

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: HBase Client Scanner Timeout exceeds Lease Period Validator

Description

Whether to suppress configuration warnings produced by the HBase Client Scanner Timeout exceeds Lease Period Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_server_scanner_rpc_timeout_validator

Required

true

Suppress Configuration Validator: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Configuration Validator: BucketCache IOEngine

Description

Whether to suppress configuration warnings produced by the BucketCache IOEngine configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_bucketcache_ioengine

Required

true

Suppress Configuration Validator: HBase Client Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the HBase Client Advanced Configuration Snippet (Safety Valve) for hbase-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_config_safety_valve

Required

true

Suppress Configuration Validator: HBase Client Environment Advanced Configuration Snippet (Safety Valve) for hbase-env.sh

Description

Whether to suppress configuration warnings produced by the HBase Client Environment Advanced Configuration Snippet (Safety Valve) for hbase-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_client_java_opts

Required

true

Suppress Configuration Validator: HBase Coprocessor Master Classes

Description

Whether to suppress configuration warnings produced by the HBase Coprocessor Master Classes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_coprocessor_master_classes

Required

true

Suppress Configuration Validator: HBase Coprocessor Region Classes

Description

Whether to suppress configuration warnings produced by the HBase Coprocessor Region Classes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_coprocessor_region_classes

Required

true

Suppress Configuration Validator: HBase HRegion Major Compaction

Description

Whether to suppress configuration warnings produced by the HBase HRegion Major Compaction configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_hregion_majorcompaction

Required

true

Suppress Configuration Validator: HBase Kerberos Secure Thrift Server Validator

Description

Whether to suppress configuration warnings produced by the HBase Kerberos Secure Thrift Server Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_kerberos_secure_thrift_validator

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for hbase-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_config_safety_valve

Required

true

Suppress Configuration Validator: HBase Master DNS Network Interface

Description

Whether to suppress configuration warnings produced by the HBase Master DNS Network Interface configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_dns_interface

Required

true

Suppress Configuration Validator: HBase Master DNS Name Server

Description

Whether to suppress configuration warnings produced by the HBase Master DNS Name Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_dns_nameserver

Required

true

Suppress Configuration Validator: HBase Master Web UI Address

Description

Whether to suppress configuration warnings produced by the HBase Master Web UI Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_info_bindaddress

Required

true

Suppress Configuration Validator: HBase Master Web UI Port

Description

Whether to suppress configuration warnings produced by the HBase Master Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_info_port

Required

true

Suppress Configuration Validator: Java Configuration Options for HBase Master

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HBase Master configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_java_opts

Required

true

Suppress Configuration Validator: Master Log Directory

Description

Whether to suppress configuration warnings produced by the Master Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_log_dir

Required

true

Suppress Configuration Validator: HBase Master Log Cleaner Plugins

Description

Whether to suppress configuration warnings produced by the HBase Master Log Cleaner Plugins configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_logcleaner_plugins

Required

true

Suppress Configuration Validator: HBase Master Port

Description

Whether to suppress configuration warnings produced by the HBase Master Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_master_port

Required

true

Suppress Configuration Validator: Netty native library working directory

Description

Whether to suppress configuration warnings produced by the Netty native library working directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_netty_native_workdir

Required

true

Suppress Configuration Validator: HBase RegionServer Interface Class

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Interface Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_class

Required

true

Suppress Configuration Validator: RegionServer Codecs

Description

Whether to suppress configuration warnings produced by the RegionServer Codecs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_codecs

Required

true

Suppress Configuration Validator: RegionServer Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the RegionServer Advanced Configuration Snippet (Safety Valve) for hbase-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_config_safety_valve

Required

true

Suppress Configuration Validator: RegionServer DNS Network Interface

Description

Whether to suppress configuration warnings produced by the RegionServer DNS Network Interface configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_dns_interface

Required

true

Suppress Configuration Validator: RegionServer DNS Nameserver

Description

Whether to suppress configuration warnings produced by the RegionServer DNS Nameserver configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_dns_nameserver

Required

true

Suppress Configuration Validator: HBase Region Server Memstore Lower Limit Validator

Description

Whether to suppress configuration warnings produced by the HBase Region Server Memstore Lower Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_global_memstore_lowerlimit_validator

Required

true

Suppress Configuration Validator: HLog Reader Implementation

Description

Whether to suppress configuration warnings produced by the HLog Reader Implementation configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_hlog_reader_impl

Required

true

Suppress Configuration Validator: HLog Writer Implementation

Description

Whether to suppress configuration warnings produced by the HLog Writer Implementation configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_hlog_writer_impl

Required

true

Suppress Configuration Validator: HBase RegionServer Web UI Address

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Web UI Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_info_bindaddress

Required

true

Suppress Configuration Validator: HBase RegionServer Web UI port

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Web UI port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_info_port

Required

true

Suppress Configuration Validator: Java Heap Size of HBase RegionServer in Bytes

Description

Whether to suppress configuration warnings produced by the Java Heap Size of HBase RegionServer in Bytes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_java_heapsize

Required

true

Suppress Configuration Validator: Java Configuration Options for HBase RegionServer

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HBase RegionServer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_java_opts

Required

true

Suppress Configuration Validator: RegionServer Log Directory

Description

Whether to suppress configuration warnings produced by the RegionServer Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_log_dir

Required

true

Suppress Configuration Validator: HBase RegionServer Multiple HDFS WAL with Replication Validator

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Multiple HDFS WAL with Replication Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_multiwal_replication_validator

Required

true

Suppress Configuration Validator: HBase RegionServer Port

Description

Whether to suppress configuration warnings produced by the HBase RegionServer Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_port

Required

true

Suppress Configuration Validator: Write-Ahead Log (WAL) Codec Class

Description

Whether to suppress configuration warnings produced by the Write-Ahead Log (WAL) Codec Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_regionserver_wal_codec

Required

true

Suppress Configuration Validator: HBase REST Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the HBase REST Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_config_safety_valve

Required

true

Suppress Configuration Validator: HBase REST Server DNS Network Interface

Description

Whether to suppress configuration warnings produced by the HBase REST Server DNS Network Interface configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_dns_interface

Required

true

Suppress Configuration Validator: HBase REST Server DNS Name Server

Description

Whether to suppress configuration warnings produced by the HBase REST Server DNS Name Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_dns_nameserver

Required

true

Suppress Configuration Validator: HBase REST Server Host Address

Description

Whether to suppress configuration warnings produced by the HBase REST Server Host Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_host

Required

true

Suppress Configuration Validator: HBase REST Server Web UI Port

Description

Whether to suppress configuration warnings produced by the HBase REST Server Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_info_port

Required

true

Suppress Configuration Validator: Java Configuration Options for HBase REST Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HBase REST Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_java_opts

Required

true

Suppress Configuration Validator: HBase REST Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HBase REST Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_file

Required

true

Suppress Configuration Validator: HBase REST Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the HBase REST Server TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_keypassword

Required

true

Suppress Configuration Validator: HBase REST Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HBase REST Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_keystore_password

Required

true

Suppress Configuration Validator: HBase REST Server Log Directory

Description

Whether to suppress configuration warnings produced by the HBase REST Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_log_dir

Required

true

Suppress Configuration Validator: HBase REST Server Port

Description

Whether to suppress configuration warnings produced by the HBase REST Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_restserver_port

Required

true

Suppress Configuration Validator: HBase Thrift Server Bind Address

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Bind Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_bindaddress

Required

true

Suppress Configuration Validator: HBase Thrift Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Advanced Configuration Snippet (Safety Valve) for hbase-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_config_safety_valve

Required

true

Suppress Configuration Validator: HBase Thrift Server DNS Network Interface

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server DNS Network Interface configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_dns_interface

Required

true

Suppress Configuration Validator: HBase Thrift Server DNS Name Server

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server DNS Name Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_dns_nameserver

Required

true

Suppress Configuration Validator: HBase Thrift Server over HTTP TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server over HTTP TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_file

Required

true

Suppress Configuration Validator: HBase Thrift Server over HTTP TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server over HTTP TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_keypassword

Required

true

Suppress Configuration Validator: HBase Thrift Server over HTTP TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server over HTTP TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_http_keystore_password

Required

true

Suppress Configuration Validator: HBase Thrift Server Web UI Port

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_info_port

Required

true

Suppress Configuration Validator: Java Configuration Options for HBase Thrift Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HBase Thrift Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_java_opts

Required

true

Suppress Configuration Validator: HBase Thrift Server Log Directory

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_log_dir

Required

true

Suppress Configuration Validator: HBase Thrift Server Port

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_thriftserver_port

Required

true

Suppress Configuration Validator: HBase REST Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HBase REST Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbaserestserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: HBase Thrift Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbasethriftserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Master Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Master Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the Rules to Extract Events from Log Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Configuration Validator: Master Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Master Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_master_role_env_safety_valve

Required

true

Suppress Configuration Validator: HBase Master TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the HBase Master TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_master_truststore_file

Required

true

Suppress Configuration Validator: HBase Master TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the HBase Master TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_master_truststore_password

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: RegionServer File Descriptor Limit Validator

Description

Whether to suppress configuration warnings produced by the RegionServer File Descriptor Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_fd_limit_validator

Required

true

Suppress Configuration Validator: RegionServer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the RegionServer Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: HBase Region Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the HBase Region Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_truststore_file

Required

true

Suppress Configuration Validator: HBase Region Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the HBase Region Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_regionserver_truststore_password

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_application_properties_safety_valve

Required

true

Suppress Parameter Validation: Atlas Kafka Messages Spool Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Kafka Messages Spool Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_message_spool_path

Required

true

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Configuration Validator: Secure Web UI Validator

Description

Whether to suppress configuration warnings produced by the Secure Web UI Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_secure_web_ui

Required

true

Suppress Configuration Validator: HBase Authentication And Authorization Validation

Description

Whether to suppress configuration warnings produced by the HBase Authentication And Authorization Validation configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_authentication_and_authorization_validator

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_core_site_safety_valve

Required

true

Suppress Parameter Validation: Dynamic Jars Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Dynamic Jars Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_dynamic_jars_dir

Required

true

Suppress Parameter Validation: HBoss S3A Implementation Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBoss S3A Implementation Class parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_hboss_fs_s3a_impl

Required

true

Suppress Parameter Validation: HBoss Lock Implementation

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBoss Lock Implementation parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_hboss_fs_sync_impl

Required

true

Suppress Parameter Validation: HBoss Wrapped S3A Implementation Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBoss Wrapped S3A Implementation Class parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_hboss_wrapped_fs_s3a_impl

Required

true

Suppress Parameter Validation: HBase Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_proxy_user_groups_list

Required

true

Suppress Parameter Validation: HBase Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: HBase Region Health Canary Exclude Tables

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Region Health Canary Exclude Tables parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_region_health_canary_exclude_tables

Required

true

Suppress Parameter Validation: HBase replication auxiliary info

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase replication auxiliary info parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_replication_auxiliary_info

Required

true

Suppress Parameter Validation: HBase replication setup status

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase replication setup status parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_replication_setup_statuses

Required

true

Suppress Parameter Validation: Assigned SPNEGO virtual groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Assigned SPNEGO virtual groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_security_authentication_spnego_admin_groups

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for hbase-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for hbase-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_service_config_safety_valve

Required

true

Suppress Parameter Validation: HBase Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_service_env_safety_valve

Required

true

Suppress Parameter Validation: HBase Snapshot Service Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Snapshot Service Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_snapshot_mapreduce_config_safety_valve

Required

true

Suppress Parameter Validation: AWS S3 Access Key ID for Remote Snapshots

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AWS S3 Access Key ID for Remote Snapshots parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_snapshot_s3_access_key_id

Required

true

Suppress Parameter Validation: AWS S3 Path for Remote Snapshots

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AWS S3 Path for Remote Snapshots parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_snapshot_s3_path

Required

true

Suppress Parameter Validation: Scheduler Pool for Remote Snapshots in AWS S3

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Scheduler Pool for Remote Snapshots in AWS S3 parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_snapshot_s3_scheduler_pool

Required

true

Suppress Parameter Validation: AWS S3 Secret Access Key for Remote Snapshots

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the AWS S3 Secret Access Key for Remote Snapshots parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_snapshot_s3_secret_access_key

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_ssl_server_safety_valve

Required

true

Suppress Parameter Validation: HBase Superusers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Superusers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_superuser

Required

true

Suppress Configuration Validator: Phoenix HBase Dynamic Jars Validator

Description

Whether to suppress configuration warnings produced by the Phoenix HBase Dynamic Jars Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_use_dynamic_jars_validator

Required

true

Suppress Parameter Validation: HBase User to Impersonate

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase User to Impersonate parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_user_to_impersonate

Required

true

Suppress Parameter Validation: HDFS WAL Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS WAL Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_wal_dir

Required

true

Suppress Configuration Validator: HBase REST Server Count Validator

Description

Whether to suppress configuration warnings produced by the HBase REST Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hbaserestserver_count_validator

Required

true

Suppress Configuration Validator: HBase Thrift Server Count Validator

Description

Whether to suppress configuration warnings produced by the HBase Thrift Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hbasethriftserver_count_validator

Required

true

Suppress Parameter Validation: HDFS Root Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Root Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_rootdir

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: Master Count Validator

Description

Whether to suppress configuration warnings produced by the Master Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_master_count_validator

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: HBASE Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBASE Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Audit Event Tracker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Tracker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_event_tracker

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Service Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_service_name

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Service Advanced Configuration Snippet (Safety Valve) for ranger-hbase-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Configuration Validator: RegionServer Count Validator

Description

Whether to suppress configuration warnings produced by the RegionServer Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_regionserver_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Configuration Validator: Short-Circuit Read Enabled Validator

Description

Whether to suppress configuration warnings produced by the Short-Circuit Read Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_short_circuit_read_validator

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: HBase TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: HBase TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: HBase TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: ZooKeeper Max Session Timeout Validator

Description

Whether to suppress configuration warnings produced by the ZooKeeper Max Session Timeout Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_max_session_timeout_validator

Required

true

Suppress Parameter Validation: ZooKeeper Znode Parent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Znode Parent parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_znode_parent

Required

true

Suppress Parameter Validation: ZooKeeper Znode Rootserver

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Znode Rootserver parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_znode_rootserver

Required

true

Suppress Health Test: HBase Master Health

Description

Whether to suppress the results of the HBase Master Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hbase_master_health

Required

true

Suppress Health Test: RegionServer Health

Description

Whether to suppress the results of the RegionServer Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hbase_region_servers_healthy

Required

true

HDFS Properties in Cloudera Runtime 7.2.18

Role groups:

Balancer

Advanced

Balancer Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

balancer_config_safety_valve

Required

false

Java Configuration Options for Balancer

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

balancer_java_opts

Required

false

Balancer Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Balancer Log Directory

Description

Directory where Balancer will place its log files.

Related Name

Default Value

/var/log/hadoop-hdfs

API Name

balancer_log_dir

Required

false

Balancer Logging Threshold

Description

The minimum log level for Balancer logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Balancer Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Balancer logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Balancer Max Log Size

Description

The maximum size, in megabytes, per log file for Balancer logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Unknown job [^]+ being deleted.* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command .+ No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Other

Dispatcher Threads

Description

Thread pool size for dispatching block moves.

Related Name

dfs.balancer.dispatcherThreads

Default Value

200

API Name

dfs_balancer_dispatcher_threads

Required

false

Minimum Block Size

Description

Smallest block to consider for moving.

Related Name

dfs.balancer.getBlocks.min-block-size

Default Value

10 MiB

API Name

dfs_balancer_get_blocks_min_block_size

Required

false

Block Metadata Batch Size

Description

Amount of block metadata to retrieve at a time.

Related Name

dfs.balancer.getBlocks.size

Default Value

2 GiB

API Name

dfs_balancer_get_blocks_size

Required

false

Maximum Concurrent Moves

Description

Number of block moves to permit in parallel.

Related Name

dfs.datanode.balance.max.concurrent.moves

Default Value

50

API Name

dfs_balancer_max_concurrent_moves

Required

false

Maximum Iteration Size

Description

Maximum amount of data to move per node in each iteration of the balancer.

Related Name

dfs.balancer.max-size-to-move

Default Value

10 GiB

API Name

dfs_balancer_max_size_to_move

Required

false

Mover Threads

Description

Thread pool size for executing block moves.

Related Name

dfs.balancer.moverThreads

Default Value

1000

API Name

dfs_balancer_mover_threads

Required

false

Excluded Hosts

Description

Hosts to exclude from the balancing process.

Related Name

Default Value

API Name

rebalancer_exclude_hosts

Required

false

Included Hosts

Description

Hosts to include in the balancing process (uses all, if none specified).

Related Name

Default Value

API Name

rebalancer_include_hosts

Required

false

Source Hosts

Description

Manual override to specify which DataNodes should be used to off-load data to less full nodes.

Related Name

Default Value

API Name

rebalancer_source_hosts

Required

false

Rebalancing Threshold

Description

The percentage deviation from average utilization, after which a node will be rebalanced. (for example, '10.0' for 10%).

Related Name

Default Value

10.0 %

API Name

rebalancer_threshold

Required

false

Rebalancing Policy

Description

The policy that should be used to rebalance HDFS storage. The default DataNode policy balances the storage at the DataNode level. This is similar to the balancing policy from prior releases. The BlockPool policy balances the storage at the block pool level as well as at the DataNode level. The BlockPool policy is relevant only to a Federated HDFS service.

Related Name

Default Value

DataNode

API Name

rebalancing_policy

Required

false

Resource Management

Java Heap Size of Balancer in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

balancer_java_heapsize

Required

false

Suppressions

Suppress Parameter Validation: Balancer Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Balancer Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_java_opts

Required

true

Suppress Parameter Validation: Balancer Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Balancer Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_log_dir

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Balancer Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Balancer Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Excluded Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Excluded Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_exclude_hosts

Required

true

Suppress Parameter Validation: Included Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Included Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_include_hosts

Required

true

Suppress Parameter Validation: Source Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Source Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_source_hosts

Required

true

DataNode

Advanced

DataNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

datanode_config_safety_valve

Required

false

Java Configuration Options for DataNode

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

datanode_java_opts

Required

false

DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

DATANODE_role_env_safety_valve

Required

false

Available Space Policy Balanced Preference

Description

Only used when the DataNode Volume Choosing Policy is set to Available Space. Controls what percentage of new block allocations will be sent to volumes with more available disk space than others. This setting should be in the range 0.0 - 1.0, though in practice 0.5 - 1.0, since there should be no reason to prefer that volumes with less available disk space receive more block allocations.

Related Name

dfs.datanode.available-space-volume-choosing-policy.balanced-space-preference-fraction

Default Value

0.75

API Name

dfs_datanode_available_space_balanced_preference

Required

true

Available Space Policy Balanced Threshold

Description

Only used when the DataNode Volume Choosing Policy is set to Available Space. Controls how much DataNode volumes are allowed to differ in terms of bytes of free disk space before they are considered imbalanced. If the free space of all the volumes are within this range of each other, the volumes will be considered balanced and block assignments will be done on a pure round robin basis.

Related Name

dfs.datanode.available-space-volume-choosing-policy.balanced-space-threshold

Default Value

10 GiB

API Name

dfs_datanode_available_space_balanced_threshold

Required

true

DataNode Volume Choosing Policy

Description

DataNode Policy for picking which volume should get a new block. The Available Space policy is only available starting with CDH 4.3.

Related Name

dfs.datanode.fsdataset.volume.choosing.policy

Default Value

org.apache.hadoop.hdfs.server.datanode.fsdataset.RoundRobinVolumeChoosingPolicy

API Name

dfs_datanode_volume_choosing_policy

Required

true

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

DataNode Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Erasure Coding

DataNode Striped Read Reconstruction Threads

Description

The number of threads that a DataNode can use during background data reconstruction.

Related Name

dfs.datanode.ec.reconstruction.threads

Default Value

20

API Name

erasure_coding_reconstruction_threads

Required

false

DataNode Striped Read Reconstruction Timeout

Description

The timeout for striped reads during background data reconstruction.

Related Name

dfs.datanode.ec.reconstruction.stripedread.timeout.millis

Default Value

5 second(s)

API Name

erasure_coding_reconstruction_timeout_millis

Required

false

Erasure Coding Reconstruction Weight

Description

The relative weight of resources used by EC for data recovery. The number of blocks that must be read is based on the EC policy used. For example, RS-6-3-1024k requires six blocks to be read. Replication only requires one block to be read. Higher values result in fewer reconstruction tasks being able to run concurrently. The number of blocks required to be read to recover data is multiplied by this weight to determine the total weight of the recovery task. The total weight of the recovery task counts against the limit set with the dfs.namenode.replication.max-streams property.

Related Name

dfs.datanode.ec.reconstruction.xmits.weight

Default Value

0.5

API Name

erasure_coding_reconstruction_xmits_weight

Required

false

Logs

DataNode Log Directory

Description

Directory where DataNode will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

datanode_log_dir

Required

false

DataNode Logging Threshold

Description

The minimum log level for DataNode logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

DataNode Maximum Log File Backups

Description

The maximum number of rolled log files to keep for DataNode logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

DataNode Max Log Size

Description

The maximum size, in megabytes, per log file for DataNode logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

DataNode Block Count Thresholds

Description

The health test thresholds of the number of blocks on a DataNode

Related Name

Default Value

Warning: 1000000.0, Critical: Never

API Name

datanode_block_count_thresholds

Required

false

DataNode Connectivity Health Test

Description

Enables the health test that verifies the DataNode is connected to the NameNode

Related Name

Default Value

true

API Name

datanode_connectivity_health_enabled

Required

false

DataNode Connectivity Tolerance at Startup

Description

The amount of time to wait for the DataNode to fully start up and connect to the NameNode before enforcing the connectivity check.

Related Name

Default Value

3 minute(s)

API Name

datanode_connectivity_tolerance

Required

false

DataNode Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's DataNode Data Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

datanode_data_directories_free_space_absolute_thresholds

Required

false

DataNode Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's DataNode Data Directory. Specified as a percentage of the capacity on that filesystem. This setting

is not used if a DataNode Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

datanode_data_directories_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

datanode_fd_thresholds

Required

false

DataNode Free Space Monitoring Thresholds

Description

The health test thresholds of free space in a DataNode. Specified as a percentage of the capacity on the DataNode.

Related Name

Default Value

Warning: 20.0 %, Critical: 10.0 %

API Name

datanode_free_space_thresholds

Required

false

DataNode Host Health Test

Description

When computing the overall DataNode health, consider the host's health.

Related Name

Default Value

true

API Name

datanode_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

datanode_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

datanode_pause_duration_window

Required

false

DataNode Process Health Test

Description

Enables the health test that the DataNode's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

datanode_scm_health_enabled

Required

false

DataNode Transceivers Usage Thresholds

Description

The health test thresholds of transceivers usage in a DataNode. Specified as a percentage of the total configured number of transceivers.

Related Name

Default Value

Warning: 75.0 %, Critical: 95.0 %

API Name

datanode_transceivers_usage_thresholds

Required

false

DataNode Volume Failures Thresholds

Description

The health test thresholds of failed volumes in a DataNode.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

datanode_volume_failures_thresholds

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

datanode_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

datanode_web_metric_collection_thresholds

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

false

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11111

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN,

content: .* is deprecated. Use .* instead , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 1, periodminutes: 5, content: Datanode registration failed , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Got a command from standby NN - ignoring command:.* , alert: false, rate: 0, threshold: WARN, content: Unknown job [^]+ being deleted.* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command . + No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls:

insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

DataNode Data Directory

Description

Comma-delimited list of directories on the local file system where the DataNode stores HDFS block data. Typical values are /data/N/dfs/dn for N = 1, 2, 3.... In CDH 5.7 and higher, these directories can be optionally tagged with their storage types, for example, [SSD]/data/1/dns/dn. HDFS supports the following storage types: [DISK], [SSD], [ARCHIVE], [RAM_DISK]. The default storage type of a directory will be [DISK] if it does not have a storage type tagged explicitly. These directories should be mounted using the noatime option, and the disks should be configured using JBOD.

RAID is not recommended. Warning: Be very careful when modifying this property. Removing or changing entries can result in data loss. To hot swap drives in CDH 5.4 and higher, override the value of this property for the specific DataNode role instance that has the drive to be hot-swapped; do not modify the property value in the role group. See Configuring Hot Swap for DataNodes for more information.

Related Name

dfs.datanode.data.dir

Default Value

API Name

dfs_data_dir_list

Required

true

Reserved Space for Non DFS Use

Description

Reserved space in bytes per volume for non Distributed File System (DFS) use.

Related Name

dfs.datanode.du.reserved

Default Value

10 GiB

API Name

dfs_datanode_du_reserved

Required

false

DataNode Failed Volumes Tolerated

Description

The number of volumes that are allowed to fail before a DataNode stops offering service. By default, any volume failure will cause a DataNode to shutdown.

Related Name

dfs.datanode.failed.volumes.tolerated

Default Value

0

API Name

dfs_datanode_failed_volumes_tolerated

Required

false

Performance

DataNode Balancing Bandwidth

Description

Maximum amount of bandwidth that each DataNode can use for balancing. Specified in bytes per second.

Related Name

dfs.datanode.balance.bandwidthPerSec

Default Value

10 MiB

API Name

dfs_balance_bandwidthPerSec

Required

false

Enable purging cache after reads

Description

In some workloads, the data read from HDFS is known to be significantly large enough that it is unlikely to be useful to cache it in the operating system buffer cache. In this case, the DataNode may be configured to automatically purge all data from the buffer cache after it is delivered to the client. This may improve performance for some workloads by freeing buffer cache spare usage for more cacheable data. This behavior will always be disabled for workloads that read only short sections of a block (e.g HBase random-IO workloads). This property is supported in CDH3u3 or later deployments.

Related Name

dfs.datanode.drop.cache.behind.reads

Default Value

false

API Name

dfs_datanode_drop_cache_behind_reads

Required

false

Enable purging cache after writes

Description

In some workloads, the data written to HDFS is known to be significantly large enough that it is unlikely to be useful to cache it in the operating system buffer cache. In this case, the DataNode may be configured to automatically purge all data from the buffer cache after it is written to disk. This may improve performance for some workloads by freeing buffer cache spare usage for more cacheable data. This property is supported in CDH3u3 or later deployments.

Related Name

dfs.datanode.drop.cache.behind.writes

Default Value

false

API Name

dfs_datanode_drop_cache_behind_writes

Required

false

Handler Count

Description

The number of server threads for the DataNode.

Related Name

dfs.datanode.handler.count

Default Value

3

API Name

dfs_datanode_handler_count

Required

false

Maximum Number of Transfer Threads

Description

Specifies the maximum number of threads to use for transferring data in and out of the DataNode.

Related Name

dfs.datanode.max.transfer.threads

Default Value

4096

API Name

dfs_datanode_max_xcievers

Required

false

Number of read ahead bytes

Description

While reading block files, the DataNode can use the posix_fadvise system call to explicitly page data into the operating system buffer cache ahead of the current reader's position. This can improve performance especially when disks are highly contended. This configuration specifies the number of bytes ahead of the current read position which the DataNode will attempt to read ahead. A value of 0 disables this feature. This property is supported in CDH3u3 or later deployments.

Related Name

dfs.datanode.readahead.bytes

Default Value

4 MiB

API Name

dfs_datanode_readahead_bytes

Required

false

Enable immediate enqueuing of data to disk after writes

Description

If this configuration is enabled, the DataNode will instruct the operating system to enqueue all written data to the disk immediately after it is written. This differs from the usual OS policy which may wait for up to 30 seconds before triggering writeback. This may improve performance for some workloads by smoothing the IO profile for data written to disk. This property is supported in CDH3u3 or later deployments.

Related Name

dfs.datanode.sync.behind.writes

Default Value

false

API Name

dfs_datanode_sync_behind_writes

Required

false

HDFS Thrift Server Max Threadcount

Description

Maximum number of running threads for the HDFS Thrift server running on each DataNode

Related Name

dfs.thrift.threads.max

Default Value

20

API Name

dfs_thrift_threads_max

Required

false

HDFS Thrift Server Min Threadcount

Description

Minimum number of running threads for the HDFS Thrift server running on each DataNode

Related Name

dfs.thrift.threads.min

Default Value

10

API Name

dfs_thrift_threads_min

Required

false

HDFS Thrift Server Timeout

Description

Timeout in seconds for the HDFS Thrift server running on each DataNode

Related Name

dfs.thrift.timeout

Default Value

60

API Name

dfs_thrift_timeout

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Bind DataNode to Wildcard Address

Description

If enabled, the DataNode binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

dfs_datanode_bind_wildcard

Required

false

DataNode HTTP Web UI Port

Description

Port for the DataNode HTTP web UI. Combined with the DataNode's hostname to build its HTTP address.

Related Name

dfs.datanode.http.address

Default Value

9864

API Name

dfs_datanode_http_port

Required

false

Secure DataNode Web UI Port (TLS/SSL)

Description

The base port where the secure DataNode web UI listens. Combined with the DataNode's hostname to build its secure web UI address.

Related Name

dfs.datanode.https.address

Default Value

9865

API Name

dfs_datanode_https_port

Required

false

DataNode Protocol Port

Description

Port for the various DataNode Protocols. Combined with the DataNode's hostname to build its IPC port address.

Related Name

dfs.datanode.ipc.address

Default Value

9867

API Name

dfs_datanode_ipc_port

Required

false

DataNode Transceiver Port

Description

Port for DataNode's XCeiver Protocol. Combined with the DataNode's hostname to build its address.

Related Name

dfs.datanode.address

Default Value

9866

API Name

dfs_datanode_port

Required

false

Use DataNode Hostname

Description

Whether DataNodes should use DataNode hostnames when connecting to DataNodes for data transfer. This property is supported in CDH3u4 or later deployments.

Related Name

dfs.datanode.use.datanode.hostname

Default Value

false

API Name

dfs_datanode_use_datanode_hostname

Required

false

Resource Management

Java Heap Size of DataNode in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

datanode_java_heapsize

Required

false

Maximum Memory Used for Caching

Description

The maximum amount of memory a DataNode may use to cache data blocks in memory. Setting it to zero will disable caching.

Related Name

dfs.datanode.max.locked.memory

Default Value

4 GiB

API Name

dfs_datanode_max_locked_memory

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

DataNode Data Directory Permissions

Description

Permissions for the directories on the local file system where the DataNode stores its blocks. The permissions must be octal. 755 and 700 are typical values.

Related Name

dfs.datanode.data.dir.perm

Default Value

700

API Name

dfs_datanode_data_dir_perm

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: DataNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_config_safety_valve

Required

true

Suppress Configuration Validator: DataNode Failed Volumes Tolerated Validator

Description

Whether to suppress configuration warnings produced by the DataNode Failed Volumes Tolerated Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_failed_volumes_validator

Required

true

Suppress Parameter Validation: Java Heap Size of DataNode in Bytes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of DataNode in Bytes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_java_heapsize

Required

true

Suppress Parameter Validation: Java Configuration Options for DataNode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for DataNode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_java_opts

Required

true

Suppress Parameter Validation: DataNode Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_log_dir

Required

true

Suppress Configuration Validator: DataNode Reserved Space Validator

Description

Whether to suppress configuration warnings produced by the DataNode Reserved Space Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_reserved_space_validator

Required

true

Suppress Parameter Validation: DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_role_env_safety_valve

Required

true

Suppress Parameter Validation: DataNode Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_data_dir_list

Required

true

Suppress Parameter Validation: DataNode Data Directory Permissions

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Data Directory Permissions parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_data_dir_perm

Required

true

Suppress Parameter Validation: DataNode HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_http_port

Required

true

Suppress Parameter Validation: Secure DataNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure DataNode Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_https_port

Required

true

Suppress Parameter Validation: DataNode Protocol Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Protocol Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_ipc_port

Required

true

Suppress Parameter Validation: DataNode Transceiver Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Transceiver Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_port

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: DataNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_audit_health

Required

true

Suppress Health Test: Block Count

Description

Whether to suppress the results of the Block Count heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_block_count

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_file_descriptor

Required

true

Suppress Health Test: Free Space

Description

Whether to suppress the results of the Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_free_space_remaining

Required

true

Suppress Health Test: NameNode Connectivity

Description

Whether to suppress the results of the NameNode Connectivity heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_ha_connectivity

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_pause_duration

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_swap_memory_usage_rate

Required

true

Suppress Health Test: Transceiver Usage

Description

Whether to suppress the results of the Transceiver Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_transceivers_usage

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_unexpected_exits

Required

true

Suppress Health Test: Data Directory Status

Description

Whether to suppress the results of the Data Directory Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_volume_failures

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_data_node_web_metric_collection

Required

true

Suppress Health Test: DataNode Data Directory Free Space

Description

Whether to suppress the results of the DataNode Data Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_datanode_data_directories_free_space

Required

true

Failover Controller

Advanced

Java Configuration Options for Failover Controller

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

failover_controller_java_opts

Required

false

Failover Controller Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

FAILOVERCONTROLLER_role_env_safety_valve

Required

false

Failover Controller Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

fc_config_safety_valve

Required

false

HA Health Monitor RPC Timeout

Description

The RPC timeout for the HA health monitor.

Related Name

ha.health-monitor.rpc-timeout.ms

Default Value

45 second(s)

API Name

ha_health_monitor_rpc_timeout_ms

Required

false

Failover Controller Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Failover Controller Log Directory

Description

Directory where Failover Controller will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

failover_controller_log_dir

Required

false

Failover Controller Logging Threshold

Description

The minimum log level for Failover Controller logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Failover Controller Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Failover Controller logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Failover Controller Max Log Size

Description

The maximum size, in megabytes, per log file for Failover Controller logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

failovercontroller_fd_thresholds

Required

false

Failover Controller Host Health Test

Description

When computing the overall Failover Controller health, consider the host's health.

Related Name

Default Value

true

API Name

failovercontroller_host_health_enabled

Required

false

Failover Controller Process Health Test

Description

Enables the health test that the Failover Controller's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

failovercontroller_scm_health_enabled

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.

- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME,

$CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.

- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Java Heap Size of Failover Controller in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

failover_controller_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Java Configuration Options for Failover Controller

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Failover Controller parameter.

Related Name

Default Value

false

API Name

role_config_suppression_failover_controller_java_opts

Required

true

Suppress Parameter Validation: Failover Controller Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Failover Controller Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_failover_controller_log_dir

Required

true

Suppress Parameter Validation: Failover Controller Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Failover Controller Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_failovercontroller_role_env_safety_valve

Required

true

Suppress Parameter Validation: Failover Controller Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Failover Controller Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fc_config_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Failover Controller Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Failover Controller Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hdfs_failovercontroller_unexpected_exits

Required

true

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hadoop

API Name

client_config_root_dir

Required

true

Short-Circuit Read Streams Cache Size

Description

The maximum number of file descriptors cached for short-circuit reads. Setting this higher will use more file descriptors, but potentially provide better performance on workloads involving lots of seeks.

Related Name

dfs.client.read.shortcircuit.streams.cache.size

Default Value

4096

API Name

dfs_client_read_shortcircuit_streams_cache_size

Required

false

HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for hdfs-site.xml.

Related Name

Default Value

API Name

hdfs_client_config_safety_valve

Required

false

HDFS Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hadoop-env.sh

Related Name

Default Value

API Name

hdfs_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

hdfs_client_java_opts

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Use Trash

Description

Move deleted files to the trash so that they can be recovered if necessary. This client side configuration takes effect only if the HDFS service-wide trash is disabled (NameNode Filesystem Trash Interval set to 0) and is ignored otherwise. The trash is not automatically emptied when enabled with this configuration.

Related Name

Default Value

false

API Name

dfs_client_use_trash

Required

false

Performance

Enable HDFS Short-Circuit Read

Description

Enable HDFS short-circuit read. This allows a client colocated with the DataNode to read HDFS file blocks directly. This gives a performance boost to distributed clients that are aware of locality.

Related Name

dfs.client.read.shortcircuit

Default Value

true

API Name

dfs_client_read_shortcircuit

Required

false

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

hdfs_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_config_safety_valve

Required

true

Suppress Parameter Validation: HDFS Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_java_opts

Required

true

Suppress Configuration Validator: HDFS Trash Enabled Validator

Description

Whether to suppress configuration warnings produced by the HDFS Trash Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_trash_disabled_validator

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

HttpFS

Advanced

HttpFS Advanced Configuration Snippet (Safety Valve) for httpfs-site.xml

Description

For advanced use only. A string to be inserted into httpfs-site.xml for this role only.

Related Name

Default Value

API Name

httpfs_config_safety_valve

Required

false

HttpFS Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

httpfs_core_site_safety_valve

Required

false

HttpFS Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

httpfs_hdfs_site_safety_valve

Required

false

Java Configuration Options for HttpFS

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

httpfs_java_opts

Required

false

System Group

Description

The group that the HttpFS server process should run as.

Related Name

Default Value

httpfs

API Name

httpfs_process_groupname

Required

true

System User

Description

The user that the HttpFS server process should run as.

Related Name

Default Value

httpfs

API Name

httpfs_process_username

Required

true

HttpFS Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HTTPFS_role_env_safety_valve

Required

false

HttpFS Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions

and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HttpFS Log Directory

Description

Directory where HttpFS will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-httpfs

API Name

httpfs_log_dir

Required

false

HttpFS Logging Threshold

Description

The minimum log level for HttpFS logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HttpFS Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HttpFS logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HttpFS Max Log Size

Description

The maximum size, in megabytes, per log file for HttpFS logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

httpfs_fd_thresholds

Required

false

HttpFS Host Health Test

Description

When computing the overall HttpFS health, consider the host's health.

Related Name

Default Value

true

API Name

httpfs_host_health_enabled

Required

false

HttpFS Process Health Test

Description

Enables the health test that the HttpFS's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

httpfs_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:

$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HttpFS Load Balancer

Description

Address of the load balancer used for HttpFS roles. Should be specified in host:port format. Note: Changing this property will regenerate Kerberos keytabs for all HttpFS roles.

Related Name

Default Value

API Name

httpfs_load_balancer

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Administration Port

Description

The port for the administration interface.

Related Name

hdfs.httpfs.admin.port

Default Value

14001

API Name

hdfs_httpfs_admin_port

Required

false

REST Port

Description

The port where the REST interface to HDFS is available. The REST interface is served over HTTPS if TLS/SSL is enabled for HttpFS, or over HTTP otherwise.

Related Name

hdfs.httpfs.http.port

Default Value

14000

API Name

hdfs_httpfs_http_port

Required

false

Resource Management

Java Heap Size of HttpFS in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

httpfs_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Signature Secret

Description

The secret to use for signing client authentication tokens.

Related Name

hdfs.httpfs.signature.secret

Default Value

******

API Name

hdfs_httpfs_signature_secret

Required

true

HttpFS TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HttpFS is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

Default Value

API Name

httpfs_https_keystore_file

Required

false

HttpFS TLS/SSL Server Keystore File Password

Description

The password for the HttpFS keystore file.

Related Name

Default Value

API Name

httpfs_https_keystore_password

Required

false

HttpFS TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HttpFS might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

httpfs_https_truststore_file

Required

false

HttpFS TLS/SSL Trust Store Password

Description

The password for the HttpFS TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

httpfs_https_truststore_password

Required

false

Enable TLS/SSL for HttpFS

Description

Encrypt communication between clients and HttpFS using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

Default Value

false

API Name

httpfs_use_ssl

Required

false

Role-Specific Kerberos Principal

Description

Kerberos principal used by the HttpFS roles.

Related Name

Default Value

httpfs

API Name

kerberos_role_princ_name

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Administration Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Administration Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_admin_port

Required

true

Suppress Parameter Validation: REST Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the REST Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_http_port

Required

true

Suppress Parameter Validation: Signature Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Signature Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_signature_secret

Required

true

Suppress Parameter Validation: HttpFS Advanced Configuration Snippet (Safety Valve) for httpfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Advanced Configuration Snippet (Safety Valve) for httpfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_config_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_core_site_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_hdfs_site_safety_valve

Required

true

Suppress Parameter Validation: HttpFS TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_keystore_file

Required

true

Suppress Parameter Validation: HttpFS TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_keystore_password

Required

true

Suppress Parameter Validation: HttpFS TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_truststore_file

Required

true

Suppress Parameter Validation: HttpFS TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_truststore_password

Required

true

Suppress Parameter Validation: Java Configuration Options for HttpFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HttpFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_java_opts

Required

true

Suppress Parameter Validation: HttpFS Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_load_balancer

Required

true

Suppress Parameter Validation: HttpFS Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_log_dir

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_process_username

Required

true

Suppress Parameter Validation: HttpFS Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: HttpFS Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_httpfs_unexpected_exits

Required

true

JournalNode

Advanced

Enable JournalNode Syncer

Description

When enabled, a JournalNode will periodically sync edit logs with other JournalNodes.

Related Name

dfs.journalnode.enable.sync

Default Value

true

API Name

dfs_journalnode_enable_sync

Required

false

JournalNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

jn_config_safety_valve

Required

false

Java Configuration Options for JournalNode

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

journalNode_java_opts

Required

false

JournalNode Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

JOURNALNODE_role_env_safety_valve

Required

false

JournalNode Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

JournalNode Log Directory

Description

Directory where JournalNode will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

journalnode_log_dir

Required

false

JournalNode Logging Threshold

Description

The minimum log level for JournalNode logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

JournalNode Maximum Log File Backups

Description

The maximum number of rolled log files to keep for JournalNode logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

JournalNode Max Log Size

Description

The maximum size, in megabytes, per log file for JournalNode logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

JournalNode Edits Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's JournalNode Edits Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

journalnode_edits_directory_free_space_absolute_thresholds

Required

false

JournalNode Edits Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's JournalNode Edits Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a JournalNode Edits Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

journalnode_edits_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

journalnode_fd_thresholds

Required

false

JournalNode Fsync Latency Thresholds

Description

The health test thresholds for JournalNode fsync latency.

Related Name

Default Value

Warning: 1 second(s), Critical: 3 second(s)

API Name

journalnode_fsync_latency_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

journalnode_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

journalnode_gc_duration_window

Required

false

JournalNode Host Health Test

Description

When computing the overall JournalNode health, consider the host's health.

Related Name

Default Value

true

API Name

journalnode_host_health_enabled

Required

false

JournalNode Process Health Test

Description

Enables the health test that the JournalNode's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

journalnode_scm_health_enabled

Required

false

Active NameNode Sync Status Health Check

Description

Enables the health check that verifies the active NameNode's sync status to the JournalNode

Related Name

Default Value

true

API Name

journalnode_sync_status_enabled

Required

false

Active NameNode Sync Status Startup Tolerance

Description

The amount of time at JournalNode startup allowed for the active NameNode to get in sync with the JournalNode.

Related Name

Default Value

3 minute(s)

API Name

journalnode_sync_status_startup_tolerance

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

journalnode_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

journalnode_web_metric_collection_thresholds

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn:

$INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

JournalNode Edits Directory

Description

Directory on the local file system where NameNode edits are written.

Related Name

dfs.journalnode.edits.dir

Default Value

API Name

dfs_journalnode_edits_dir

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

JournalNode HTTP Port

Description

Port for the JournalNode HTTP web UI. Combined with the JournalNode hostname to build its HTTP address.

Related Name

dfs.journalnode.http-address

Default Value

8480

API Name

dfs_journalnode_http_port

Required

false

Secure JournalNode Web UI Port (TLS/SSL)

Description

The base port where the secure JournalNode web UI listens. Combined with the JournalNode's hostname to build its secure web UI address.

Related Name

dfs.journalnode.https-address

Default Value

8481

API Name

dfs_journalnode_https_port

Required

false

JournalNode RPC Port

Description

Port for the JournalNode's RPC. Combined with the JournalNode's hostname to build its RPC address.

Related Name

dfs.journalnode.rpc-address

Default Value

8485

API Name

dfs_journalnode_rpc_port

Required

false

Bind JournalNode to Wildcard Address

Description

If enabled, the JournalNode binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

journalnode_bind_wildcard

Required

false

Resource Management

Java Heap Size of JournalNode in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

512 MiB

API Name

journalNode_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JournalNode Edits Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode Edits Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_edits_dir

Required

true

Suppress Parameter Validation: JournalNode HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_http_port

Required

true

Suppress Parameter Validation: Secure JournalNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure JournalNode Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_https_port

Required

true

Suppress Parameter Validation: JournalNode RPC Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode RPC Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_rpc_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: JournalNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jn_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for JournalNode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for JournalNode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_java_opts

Required

true

Suppress Parameter Validation: JournalNode Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_log_dir

Required

true

Suppress Parameter Validation: JournalNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_role_env_safety_valve

Required

true

Suppress Parameter Validation: JournalNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JournalNode Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_audit_health

Required

true

Suppress Health Test: JournalNode Edits Directory Free Space

Description

Whether to suppress the results of the JournalNode Edits Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_edits_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_file_descriptor

Required

true

Suppress Health Test: Fsync Latency

Description

Whether to suppress the results of the Fsync Latency heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_fsync_latency

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_swap_memory_usage_rate

Required

true

Suppress Health Test: Sync Status

Description

Whether to suppress the results of the Sync Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_sync_status

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_journal_node_web_metric_collection

Required

true

NameNode

Advanced

Enable Automatic Failover

Description

Enable Automatic Failover to maintain High Availability. Requires a ZooKeeper service and a High Availability NameNode partner.

Related Name

dfs.ha.automatic-failover.enabled

Default Value

false

API Name

autofailover_enabled

Required

false

NameNode Nameservice

Description

Nameservice of this NameNode. The Nameservice represents the interface to this NameNode and its High Availability partner. The Nameservice also represents the namespace associated with a federated NameNode.

Related Name

Default Value

API Name

dfs_federation_namenode_nameservice

Required

false

Enable Async Audit Log

Description

When enabled, HDFS NameNode will append audit log asynchronously when using HDFS default audit logger. Enabling this should improve NameNode throughput under heavy load.

Related Name

dfs.namenode.audit.log.async

Default Value

true

API Name

dfs_namenode_audit_log_async

Required

false

Avoid Reading Stale DataNode

Description

Indicate whether or not to avoid reading from stale DataNodes for which heartbeat messages have not been received by the NameNode for more than Stale DataNode Time

Interval. Stale DataNodes are moved to the end of the node list returned for reading. See dfs.namenode.avoid.write.stale.datanode for a similar setting for writes.

Related Name

dfs.namenode.avoid.read.stale.datanode

Default Value

true

API Name

dfs_namenode_avoid_read_stale_datanode

Required

false

Avoid Writing Stale DataNode

Description

Indicate whether or not to avoid writing to stale DataNodes for which heartbeat messages have not been received by the NameNode for more than Stale DataNode Time Interval. Writes avoid using stale DataNodes unless more than a configured ratio (dfs.namenode.write.stale.datanode.ratio) of DataNodes are marked as stale. See dfs.namenode.avoid.read.stale.datanode for a similar setting for reads.

Related Name

dfs.namenode.avoid.write.stale.datanode

Default Value

true

API Name

dfs_namenode_avoid_write_stale_datanode

Required

false

NameNode Max Component Length

Description

Defines the maximum number of bytes in UTF-8 encoding in each component of a path. A value of 0 will disable the check.

Related Name

dfs.namenode.fs-limits.max-component-length

Default Value

255

API Name

dfs_namenode_fs_limits_max_length

Required

false

Invalidate Work Percentage Per Iteration

Description

This determines the percentage amount of block invalidations (deletes) to do over a single DataNode heartbeat deletion command. The final deletion count is determined by applying this percentage to the number of live nodes in the system. The resultant number is the number of blocks from the deletion list chosen for proper invalidation over a single heartbeat of a single DataNode.

Related Name

dfs.namenode.invalidate.work.pct.per.iteration

Default Value

0.32

API Name

dfs_namenode_invalidate_work_pct_per_iteration

Required

false

Quorum-based Storage Journal name

Description

Name of the journal located on each JournalNode filesystem.

Related Name

Default Value

API Name

dfs_namenode_quorum_journal_name

Required

false

Maximum Number of Replication Threads on a DataNode

Description

The maximum number of outgoing replication threads a node can have at one time. This limit is waived for the highest priority replications. Configure dfs.namenode.replication.max-streams-hard-limit to set the absolute limit, including the highest-priority replications.

Related Name

dfs.namenode.replication.max-streams

Default Value

20

API Name

dfs_namenode_replication_max_streams

Required

false

Hard Limit on the Number of Replication Threads on a Datanode

Description

The absolute maximum number of outgoing replication threads a given node can have at one time. The regular limit (dfs.namenode.replication.max-streams) is waived for highest-priority block replications. Highest replication priority is for blocks that are at a very high risk of loss if the disk or server on which they remain fails. These are usually blocks with only one copy, or blocks with zero live copies but a copy in a node being decommissioned. dfs.namenode.replication.max-streams-hard-limit provides a limit on the total number of outgoing replication threads, including threads of all priorities.

Related Name

dfs.namenode.replication.max-streams-hard-limit

Default Value

40

API Name

dfs_namenode_replication_max_streams_hard_limit

Required

false

Replication Work Multiplier Per Iteration

Description

This determines the total amount of block transfers to begin in parallel at a DataNode for replication, when such a command list is being sent over a DataNode heartbeat by the NameNode. The actual number is obtained by multiplying this value by the total number of live nodes in the cluster. The result number is the number of blocks to transfer immediately, per DataNode heartbeat.

Related Name

dfs.namenode.replication.work.multiplier.per.iteration

Default Value

10

API Name

dfs_namenode_replication_work_multiplier_per_iteration

Required

false

Enable Immutable Snapshots

Description

When enabled, HDFS snapshots will capture point-in-time copies of open files.

Related Name

dfs.namenode.snapshot.capture.openfiles

Default Value

true

API Name

dfs_namenode_snapshot_capture_openfiles

Required

false

Stale DataNode Time Interval

Description

Default time interval for marking a DataNode as "stale". If the NameNode has not received heartbeat messages from a DataNode for more than this time interval, the DataNode is marked and treated as "stale" by default.

Related Name

dfs.namenode.stale.datanode.interval

Default Value

30 second(s)

API Name

dfs_namenode_stale_datanode_interval

Required

false

Write Stale DataNode Ratio

Description

When the ratio of number stale DataNodes to total DataNodes marked is greater than this ratio, permit writing to stale nodes to prevent causing hotspots.

Related Name

dfs.namenode.write.stale.datanode.ratio

Default Value

0.5

API Name

dfs_namenode_write_stale_datanode_ratio

Required

false

JournalNode Accept Recovery Timeout

Description

Timeout when accepting recovery of an edit segment from JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.accept-recovery.timeout.ms

Default Value

2 minute(s)

API Name

dfs_qjournal_accept_recovery_timeout_ms

Required

false

JournalNode Finalize Segment Timeout

Description

Timeout when finalizing current edit segment with JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.finalize-segment.timeout.ms

Default Value

2 minute(s)

API Name

dfs_qjournal_finalize_segment_timeout_ms

Required

false

JournalNode Get State Timeout

Description

Timeout when getting current states from JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.get-journal-state.timeout.ms

Default Value

2 minute(s)

API Name

dfs_qjournal_get_journal_state_timeout_ms

Required

false

JournalNode New Epoch Timeout

Description

Timeout when creating new epoch number with JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.new-epoch.timeout.ms

Default Value

2 minute(s)

API Name

dfs_qjournal_new_epoch_timeout_ms

Required

false

JournalNode Prepare Recovery Timeout

Description

Timeout when preparing recovery of an edit segment with JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.prepare-recovery.timeout.ms

Default Value

2 minute(s)

API Name

dfs_qjournal_prepare_recovery_timeout_ms

Required

false

JournalNode Select Input Streams Timeout

Description

Timeout when selecting input streams on JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.select-input-streams.timeout.ms

Default Value

20 second(s)

API Name

dfs_qjournal_select_input_streams_timeout_ms

Required

false

JournalNode Start Segment Timeout

Description

Timeout when starting a new edit segment with JournalNodes. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.start-segment.timeout.ms

Default Value

20 second(s)

API Name

dfs_qjournal_start_segment_timeout_ms

Required

false

JournalNode Write Transactions Timeout

Description

Timeout when writing edits to a JournalNode. This only applies when NameNode high availability is enabled.

Related Name

dfs.qjournal.write-txns.timeout.ms

Default Value

20 second(s)

API Name

dfs_qjournal_write_txns_timeout_ms

Required

false

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

NameNode Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

NameNode Advanced Configuration Snippet (Safety Valve) for dfs_all_hosts.txt

Description

For advanced use only. A string to be inserted into dfs_all_hosts.txt for this role only.

Related Name

Default Value

API Name

namenode_all_hosts_safety_valve

Required

false

NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

namenode_config_safety_valve

Required

false

NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_allow.txt

Description

For advanced use only. A string to be inserted into dfs_hosts_allow.txt for this role only.

Related Name

Default Value

API Name

namenode_hosts_allow_safety_valve

Required

false

NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_exclude.txt

Description

For advanced use only. A string to be inserted into dfs_hosts_exclude.txt for this role only.

Related Name

Default Value

API Name

namenode_hosts_exclude_safety_valve

Required

false

Java Configuration Options for NameNode

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

namenode_java_opts

Required

false

NameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

NAMENODE_role_env_safety_valve

Required

false

Mount Points

Description

Mount points that are mapped to this NameNode's nameservice.

Related Name

Default Value

/

API Name

nameservice_mountpoints

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml

Description

For advanced use only. A string to be inserted into ranger-hdfs-security.xml for this role only.

Related Name

Default Value

API Name

ranger_security_role_safety_valve

Required

false

Checkpointing

Filesystem Checkpoint Period

Description

The time between two periodic file system checkpoints.

Related Name

dfs.namenode.checkpoint.period

Default Value

1 hour(s)

API Name

fs_checkpoint_period

Required

false

Filesystem Checkpoint Transaction Threshold

Description

The number of transactions after which the NameNode or SecondaryNameNode will create a checkpoint of the namespace, regardless of whether the checkpoint period has expired.

Related Name

dfs.namenode.checkpoint.txns

Default Value

1000000

API Name

fs_checkpoint_txns

Required

false

Erasure Coding

Fallback Erasure Coding Policy

Description

The fallback Erasure Coding policy that HDFS uses if no policy is specified when you run the -setPolicy command.

Related Name

dfs.namenode.ec.system.default.policy

Default Value

RS-6-3-1024k

API Name

erasure_coding_default_policy

Required

false

Logs

NameNode Logging Threshold

Description

The minimum log level for NameNode logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

NameNode Maximum Log File Backups

Description

The maximum number of rolled log files to keep for NameNode logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

NameNode Max Log Size

Description

The maximum size, in megabytes, per log file for NameNode logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

NameNode Block State Change Logging Threshold

Description

The minimum log level for NameNode block state change log messages. Setting this to WARN or higher greatly reduces the amount of log output related to block state changes.

Related Name

log4j.logger.BlockStateChange

Default Value

INFO

API Name

namenode_blockstatechange_log_threshold

Required

false

NameNode Log Directory

Description

Directory where NameNode will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

namenode_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11110

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Unknown job [^]+ being deleted.* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command .+ No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN , alert: false, rate: 1, threshold: INFO, content: Triggering checkpoint.*]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.

- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Filesystem Checkpoint Age Monitoring Thresholds

Description

The health test thresholds of the age of the HDFS namespace checkpoint. Specified as a percentage of the configured checkpoint interval.

Related Name

Default Value

Warning: 200.0 %, Critical: 400.0 %

API Name

namenode_checkpoint_age_thresholds

Required

false

Filesystem Checkpoint Transactions Monitoring Thresholds

Description

The health test thresholds of the number of transactions since the last HDFS namespace checkpoint. Specified as a percentage of the configured checkpointing transaction limit.

Related Name

Default Value

Warning: 200.0 %, Critical: 400.0 %

API Name

namenode_checkpoint_transactions_thresholds

Required

false

NameNode Data Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NameNode Data Directories.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

namenode_data_directories_free_space_absolute_thresholds

Required

false

NameNode Data Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NameNode Data Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NameNode Data Directories Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

namenode_data_directories_free_space_percentage_thresholds

Required

false

NameNode Directory Failures Thresholds

Description

The health test thresholds of failed status directories in a NameNode.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

namenode_directory_failures_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

namenode_fd_thresholds

Required

false

NameNode Host Health Test

Description

When computing the overall NameNode health, consider the host's health.

Related Name

Default Value

true

API Name

namenode_host_health_enabled

Required

false

NameNode Out-Of-Sync JournalNodes Thresholds

Description

The health check thresholds for the number of out-of-sync JournalNodes for this NameNode.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

namenode_out_of_sync_journal_nodes_thresholds

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

namenode_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

namenode_pause_duration_window

Required

false

HDFS Rolling Metadata Upgrade Status Health Test

Description

Enables the health test of the rolling metadata upgrade status of the NameNode. This covers rolling metadata upgrades. Nonrolling metadata upgrades are covered in a separate health test.

Related Name

Default Value

true

API Name

namenode_rolling_upgrade_status_enabled

Required

false

NameNode RPC Latency Thresholds

Description

The health check thresholds of the NameNode's RPC latency.

Related Name

Default Value

Warning: 1 second(s), Critical: 5 second(s)

API Name

namenode_rpc_latency_thresholds

Required

false

NameNode RPC Latency Monitoring Window

Description

The period to review when computing the moving average of the NameNode's RPC latency.

Related Name

Default Value

5 minute(s)

API Name

namenode_rpc_latency_window

Required

false

NameNode Safemode Health Test

Description

Enables the health test that the NameNode is not in safemode

Related Name

Default Value

true

API Name

namenode_safe_mode_enabled

Required

false

NameNode Process Health Test

Description

Enables the health test that the NameNode's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

namenode_scm_health_enabled

Required

false

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Related Name

Default Value

5 minute(s)

API Name

namenode_startup_tolerance

Required

false

HDFS Metadata Upgrade Status Health Test

Description

Enables the health test of the metadata upgrade status of the NameNode. This covers nonrolling metadata upgrades. Rolling metadata upgrades are covered in a separate health test.

Related Name

Default Value

true

API Name

namenode_upgrade_status_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

namenode_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

namenode_web_metric_collection_thresholds

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost: $ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Backup and Disaster Log Retention

Description

Maximum age of log files related to backup and disaster recovery.

Related Name

Default Value

90 day(s)

API Name

bdr_log_expiration_days

Required

false

Decommissioning blocks per interval

Description

The approximate number of blocks to process per decommission interval, as defined in dfs.namenode.decommission.interval.

Related Name

dfs.namenode.decommission.blocks.per.interval

Default Value

500000

API Name

dfs_decommission_blocks_per_interval

Required

false

Decommissioning max tracked nodes

Description

The maximum number of decommission-in-progress datanodes nodes that will be tracked at one time by the namenode. Tracking a decommission-in-progress datanode consumes additional NN memory proportional to the number of blocks on the datnode. A value of 0 means no limit will be enforced.

Related Name

dfs.namenode.decommission.max.concurrent.tracked.nodes

Default Value

100

API Name

dfs_decommission_max_concurrent_tracked_nodes

Required

false

NameNode Data Directories

Description

Determines where on the local file system the NameNode should store the name table (fsimage). For redundancy, enter a comma-delimited list of directories to replicate the name table in all of the directories. Typical values are /data/N/dfs/nn where N=1..3.

Related Name

dfs.namenode.name.dir

Default Value

API Name

dfs_name_dir_list

Required

true

Restore NameNode Directories at Checkpoint Time

Description

If set to false and if one of the replicas of the NameNode storage fails, such as temporarily failure of NFS, this directory is not used until the NameNode restarts. If enabled, failed storage is re-checked on every checkpoint and, if it becomes valid, the NameNode will try to restore the edits and fsimage.

Related Name

dfs.namenode.name.dir.restore

Default Value

true

API Name

dfs_name_dir_restore

Required

false

NameNode Edits Directories

Description

Directories on the local file system to store the NameNode edits. If not set, the edits are stored in the NameNode's Data Directories. The value of this configuration is automatically generated to be the Quorum-based Storage URI if there are JournalNodes and this NameNode is not Highly Available.

Related Name

dfs.namenode.edits.dir

Default Value

API Name

dfs_namenode_edits_dir

Required

false

Shared Edits Directory

Description

Directory on a shared storage device, such as a Quorum-based Storage URI or a local directory that is an NFS mount from a NAS, to store the NameNode edits. The value of this configuration is automatically generated to be the Quourm Journal URI if there are JournalNodes and this NameNode is Highly Available.

Related Name

dfs.namenode.shared.edits.dir

Default Value

API Name

dfs_namenode_shared_edits_dir

Required

false

Safemode Extension

Description

Determines extension of safemode in milliseconds after the threshold level is reached.

Related Name

dfs.namenode.safemode.extension

Default Value

30 second(s)

API Name

dfs_safemode_extension

Required

false

Safemode Minimum DataNodes

Description

Specifies the number of DataNodes that must be live before the name node exits safemode. Enter a value less than or equal to 0 to take the number of live DataNodes into account when deciding whether to remain in safemode during startup. Values greater than the number of DataNodes in the cluster will make safemode permanent.

Related Name

dfs.namenode.safemode.min.datanodes

Default Value

1

API Name

dfs_safemode_min_datanodes

Required

false

Filesystem Trash Checkpoint Interval

Description

Number of minutes between trash checkpoints. After a .Trash directory checkpoint is created, the Filesystem Trash Interval will define the time until permanent deletion. If set to 0, the value will be considered equal to the Filesytem Trash Interval value, which can cause the permanent deletion of entries in Trash to take over twice as long. The value for this must not exceed the Filesystem Trash Interval value.

Related Name

fs.trash.checkpoint.interval

Default Value

1 hour(s)

API Name

fs_trash_checkpoint_interval

Required

false

Filesystem Trash Interval

Description

Controls the number of minutes after which a trash checkpoint directory is deleted permanently. To disable the trash feature, enter 0. The checkpointing frequency of .Trash directory contents is separately controlled by Filesystem Trash Checkpoint Interval.

Related Name

fs.trash.interval

Default Value

1 day(s)

API Name

fs_trash_interval

Required

false

Topology Script File Name

Description

Full path to a custom topology script on the host file system. The topology script is used to determine the rack location of nodes. If left blank, a topology script will be provided that uses your hosts' rack information, visible in the "Hosts" page.

Related Name

net.topology.script.file.name

Default Value

API Name

topology_script_file_name

Required

false

Performance

NameNode Handler Count

Description

The number of server threads for the NameNode.

Related Name

dfs.namenode.handler.count

Default Value

30

API Name

dfs_namenode_handler_count

Required

false

NameNode Service Handler Count

Description

The number of server threads for the NameNode used for service calls. Only used when NameNode Service RPC Port is configured.

Related Name

dfs.namenode.service.handler.count

Default Value

30

API Name

dfs_namenode_service_handler_count

Required

false

HDFS Thrift Server Max Threadcount

Description

Maximum number of running threads for the HDFS Thrift server running on the NameNode

Related Name

dfs.thrift.threads.max

Default Value

20

API Name

dfs_thrift_threads_max

Required

false

HDFS Thrift Server Min Threadcount

Description

Minimum number of running threads for the HDFS Thrift server running on the NameNode

Related Name

dfs.thrift.threads.min

Default Value

10

API Name

dfs_thrift_threads_min

Required

false

HDFS Thrift Server Timeout

Description

Timeout in seconds for the HDFS Thrift server running on the NameNode

Related Name

dfs.thrift.timeout

Default Value

60

API Name

dfs_thrift_timeout

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

NameNode Web UI Port

Description

The base port where the DFS NameNode web UI listens. If the port number is 0, then the server starts on a free port. Combined with the NameNode's hostname to build its HTTP address.

Related Name

dfs.namenode.http-address

Default Value

9870

API Name

dfs_http_port

Required

false

Secure NameNode Web UI Port (TLS/SSL)

Description

The base port where the secure NameNode web UI listens.

Related Name

dfs.https.port

Default Value

9871

API Name

dfs_https_port

Required

false

NameNode Service RPC Port

Description

Optional port for the service-rpc address which can be used by HDFS daemons instead of sharing the RPC address used by the clients.

Related Name

dfs.namenode.servicerpc-address

Default Value

API Name

dfs_namenode_servicerpc_address

Required

false

Bind NameNode to Wildcard Address

Description

If enabled, the NameNode binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

namenode_bind_wildcard

Required

false

NameNode Port

Description

The port where the NameNode runs the HDFS protocol. Combined with the NameNode's hostname to build its address.

Related Name

fs.defaultFS

Default Value

8020

API Name

namenode_port

Required

false

Replication

Safemode Threshold Percentage

Description

Specifies the percentage of blocks that should satisfy the minimal replication requirement defined by dfs.replication.min. Enter a value less than or equal to 0 to wait for any particular percentage of blocks before exiting safemode. Values greater than 1 will make safemode permanent.

Related Name

dfs.namenode.safemode.threshold-pct

Default Value

0.999

API Name

dfs_safemode_threshold_pct

Required

false

Resource Management

Java Heap Size of NameNode in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

namenode_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Include Caller Context in Audit Logs

Description

When enabled, additional fields are written into NameNode audit log records for auditing coarse granularity operations.

Related Name

hadoop.caller.context.enabled

Default Value

true

API Name

hadoop_caller_context_enabled

Required

false

HDFS NameNode TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HDFS NameNode might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

namenode_truststore_file

Required

false

HDFS NameNode TLS/SSL Trust Store Password

Description

The password for the HDFS NameNode TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

namenode_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: NameNode Nameservice

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Nameservice parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_federation_namenode_nameservice

Required

true

Suppress Parameter Validation: NameNode Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_http_port

Required

true

Suppress Parameter Validation: Secure NameNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure NameNode Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_https_port

Required

true

Suppress Parameter Validation: NameNode Data Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Data Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_name_dir_list

Required

true

Suppress Parameter Validation: NameNode Edits Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Edits Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_edits_dir

Required

true

Suppress Configuration Validator: NameNode Handler Count Minimum Validator

Description

Whether to suppress configuration warnings produced by the NameNode Handler Count Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_handler_count_minimum_validator

Required

true

Suppress Parameter Validation: Quorum-based Storage Journal name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Quorum-based Storage Journal name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_quorum_journal_name

Required

true

Suppress Configuration Validator: NameNode Service Handler Count Minimum Validator

Description

Whether to suppress configuration warnings produced by the NameNode Service Handler Count Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_service_handler_count_minimum_validator

Required

true

Suppress Parameter Validation: NameNode Service RPC Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Service RPC Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_servicerpc_address

Required

true

Suppress Parameter Validation: Shared Edits Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Shared Edits Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_shared_edits_dir

Required

true

Suppress Configuration Validator: Filesystem Trash Interval On Validator

Description

Whether to suppress configuration warnings produced by the Filesystem Trash Interval On Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fs_trash_interval_minimum_validator

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: NameNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_all_hosts.txt

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_all_hosts.txt parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_all_hosts_safety_valve

Required

true

Suppress Parameter Validation: NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_config_safety_valve

Required

true

Suppress Parameter Validation: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_allow.txt

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_allow.txt parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_hosts_allow_safety_valve

Required

true

Suppress Parameter Validation: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_exclude.txt

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_exclude.txt parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_hosts_exclude_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of NameNode in Bytes Minimum Validator

Description

Whether to suppress configuration warnings produced by the Java Heap Size of NameNode in Bytes Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_java_heapsize_minimum_validator

Required

true

Suppress Parameter Validation: Java Configuration Options for NameNode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for NameNode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_java_opts

Required

true

Suppress Parameter Validation: NameNode Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_log_dir

Required

true

Suppress Parameter Validation: NameNode Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_port

Required

true

Suppress Parameter Validation: NameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_role_env_safety_valve

Required

true

Suppress Parameter Validation: HDFS NameNode TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS NameNode TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_truststore_file

Required

true

Suppress Parameter Validation: HDFS NameNode TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS NameNode TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_truststore_password

Required

true

Suppress Configuration Validator: Validates Nameservices do not conflict between base and compute clusters.

Description

Whether to suppress configuration warnings produced by the Validates Nameservices do not conflict between base and compute clusters. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nameservice_conflict_validator

Required

true

Suppress Parameter Validation: Mount Points

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mount Points parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nameservice_mountpoints

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_security_role_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Topology Script File Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Topology Script File Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_topology_script_file_name

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_audit_health

Required

true

Suppress Health Test: NameNode Data Directories Free Space

Description

Whether to suppress the results of the NameNode Data Directories Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_data_directories_free_space

Required

true

Suppress Health Test: Name Directory Status

Description

Whether to suppress the results of the Name Directory Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_directory_failures

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_file_descriptor

Required

true

Suppress Health Test: Checkpoint Status

Description

Whether to suppress the results of the Checkpoint Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_ha_checkpoint_age

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_host_health

Required

true

Suppress Health Test: JournalNode Sync Status

Description

Whether to suppress the results of the JournalNode Sync Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_journal_node_sync_status

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_pause_duration

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Rolling Upgrade Status

Description

Whether to suppress the results of the Rolling Upgrade Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_rolling_upgrade_status

Required

true

Suppress Health Test: RPC Latency

Description

Whether to suppress the results of the RPC Latency heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_rpc_latency

Required

true

Suppress Health Test: Safe Mode Status

Description

Whether to suppress the results of the Safe Mode Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_safe_mode

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_unexpected_exits

Required

true

Suppress Health Test: Upgrade Status

Description

Whether to suppress the results of the Upgrade Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_upgrade_status

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_name_node_web_metric_collection

Required

true

NFS Gateway

Advanced

NFS Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

NFS Gateway Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

nfsgateway_config_safety_valve

Required

false

Java Configuration Options for NFS Gateway

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

nfsgateway_java_opts

Required

false

NFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

NFSGATEWAY_role_env_safety_valve

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

NFS Gateway Logging Threshold

Description

The minimum log level for NFS Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

NFS Gateway Maximum Log File Backups

Description

The maximum number of rolled log files to keep for NFS Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

NFS Gateway Max Log Size

Description

The maximum size, in megabytes, per log file for NFS Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

NFS Gateway Log Directory

Description

Directory where NFS Gateway will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

nfsgateway_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Temporary Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Temporary Dump Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

nfsgateway_dump_directory_free_space_absolute_thresholds

Required

false

Temporary Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Temporary Dump Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Temporary Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

nfsgateway_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

nfsgateway_fd_thresholds

Required

false

NFS Gateway Host Health Test

Description

When computing the overall NFS Gateway health, consider the host's health.

Related Name

Default Value

true

API Name

nfsgateway_host_health_enabled

Required

false

NFS Gateway Process Health Test

Description

Enables the health test that the NFS Gateway's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

nfsgateway_scm_health_enabled

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:

$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Temporary Dump Directory

Description

NFS clients often reorder writes. As a result, sequential writes can arrive at the NFS Gateway in random order. This directory is used to temporarily save out-of-order writes before writing to HDFS. For each file, the out-of-order writes are dumped after they are accumulated to exceed certain threshold (e.g., 1MB) in memory. Please make sure this directory has enough space. For example, if the application uploads 10 files with each having 100MB, it is recommended that this directory have roughly 1GB of space in case write reorder happens (in the worst case) to every file.

Related Name

dfs.nfs3.dump.dir

Default Value

/tmp/.hdfs-nfs

API Name

dfs_nfs3_dump_dir

Required

false

Allowed Hosts and Privileges

Description

By default, NFS Gateway exported directories can be mounted by any client. For better access control, update this property with a list of host names and access privileges separated by whitespace characters. Host name format can be a single host, a Java regular expression, or an IPv4 address. The access privilege uses rw to specify readwrite and ro to specify readonly access. If the access privilege is not provided, the default is read-only. Examples of host name format and access privilege: "192.168.0.0/22 rw", "host.*.example.com", "host1.test.org ro".

Related Name

dfs.nfs.exports.allowed.hosts

Default Value

* rw

API Name

dfs_nfs_exports_allowed_hosts

Required

false

NFS Gateway Export Point

Description

The NFS Gateway export point(s). Full path is required. In federated clusters, multiple export points can be configured, and at most 1 export point per federated nameservice is allowed.

Related Name

nfs.export.point

Default Value

API Name

nfs_export_point

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

NFS Gateway Web UI Port

Description

The base port where the NFS Gateway server web UI listens. Combined with the NFS Gateway server hostname to build its HTTP address.

Related Name

nfs.http.port

Default Value

50079

API Name

nfs3_http_port

Required

false

Secure NFS Gateway Web UI Port (TLS/SSL)

Description

The base port where the secure NFS Gateway server web UI listens. Combined with the NFS Gateway server's hostname to build its secure web UI address.

Related Name

nfs.https.port

Default Value

50579

API Name

nfs3_https_port

Required

false

NFS Gateway MountD Port

Description

The port number of the mount daemon implemented inside the NFS Gateway server role.

Related Name

nfs3.mountd.port

Default Value

4242

API Name

nfs3_mountd_port

Required

false

Portmap (or Rpcbind) Port

Description

The port number of the system portmap or rpcbind service. This configuration is used by Cloudera Manager to verify if the system portmap or rpcbind service is running before starting NFS Gateway role. Cloudera Manager does not manage the system portmap or rpcbind service.

Related Name

Default Value

111

API Name

nfs3_portmap_port

Required

false

NFS Gateway Server Port

Description

The NFS Gateway server port.

Related Name

nfs3.server.port

Default Value

2049

API Name

nfs3_server_port

Required

false

Resource Management

Java Heap Size of NFS Gateway in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

nfsgateway_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Temporary Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Temporary Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_nfs3_dump_dir

Required

true

Suppress Parameter Validation: Allowed Hosts and Privileges

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Hosts and Privileges parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_nfs_exports_allowed_hosts

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: NFS Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: NFS Gateway Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_http_port

Required

true

Suppress Parameter Validation: Secure NFS Gateway Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure NFS Gateway Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_https_port

Required

true

Suppress Parameter Validation: NFS Gateway MountD Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway MountD Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_mountd_port

Required

true

Suppress Parameter Validation: Portmap (or Rpcbind) Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Portmap (or Rpcbind) Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_portmap_port

Required

true

Suppress Parameter Validation: NFS Gateway Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_server_port

Required

true

Suppress Parameter Validation: NFS Gateway Export Point

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Export Point parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfs_export_point

Required

true

Suppress Parameter Validation: NFS Gateway Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for NFS Gateway

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for NFS Gateway parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_java_opts

Required

true

Suppress Parameter Validation: NFS Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_log_dir

Required

true

Suppress Parameter Validation: NFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NFS Gateway Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_role_env_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_audit_health

Required

true

Suppress Health Test: Temporary Dump Directory Free Space

Description

Whether to suppress the results of the Temporary Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_dump_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nfsgateway_unexpected_exits

Required

true

SecondaryNameNode

Advanced

SecondaryNameNode Nameservice

Description

Nameservice of this SecondaryNameNode

Related Name

Default Value

API Name

dfs_secondarynamenode_nameservice

Required

false

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

SecondaryNameNode Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

SecondaryNameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only. A string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

secondarynamenode_config_safety_valve

Required

false

Java Configuration Options for Secondary NameNode

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

secondarynamenode_java_opts

Required

false

SecondaryNameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SECONDARYNAMENODE_role_env_safety_valve

Required

false

Checkpointing

Filesystem Checkpoint Period

Description

The time between two periodic file system checkpoints.

Related Name

dfs.namenode.checkpoint.period

Default Value

1 hour(s)

API Name

fs_checkpoint_period

Required

false

Filesystem Checkpoint Transaction Threshold

Description

The number of transactions after which the NameNode or SecondaryNameNode will create a checkpoint of the namespace, regardless of whether the checkpoint period has expired.

Related Name

dfs.namenode.checkpoint.txns

Default Value

1000000

API Name

fs_checkpoint_txns

Required

false

Logs

SecondaryNameNode Logging Threshold

Description

The minimum log level for SecondaryNameNode logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

SecondaryNameNode Maximum Log File Backups

Description

The maximum number of rolled log files to keep for SecondaryNameNode logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

SecondaryNameNode Max Log Size

Description

The maximum size, in megabytes, per log file for SecondaryNameNode logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

SecondaryNameNode Log Directory

Description

Directory where SecondaryNameNode will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-hdfs

API Name

secondarynamenode_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11112

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 0, exceptiontype: java.io.IOException , alert: false, rate: 0, exceptiontype: java.net.SocketException , alert: false, rate: 0, exceptiontype: java.net.SocketClosedException , alert: false, rate: 0, exceptiontype: java.io.EOFException , alert: false, rate: 0, exceptiontype: java.nio.channels.CancelledKeyException , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 0, threshold: WARN, content: Unknown job [^]+ being deleted.* , alert: false, rate: 0, threshold: WARN, content: Error executing shell command .+ No such process.+ , alert: false, rate: 0, threshold: WARN, content: .*attempt to override final parameter.+ , alert: false, rate: 0, threshold: WARN, content: [^]+ is a deprecated filesystem name. Use.* , alert: false, rate: 1, periodminutes: 1, threshold: WARN , alert: false, rate: 1, threshold: INFO, content: Triggering checkpoint.*]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.

- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

HDFS Checkpoint Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's HDFS Checkpoint Directories.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

secondarynamenode_checkpoint_directories_free_space_absolute_thresholds

Required

false

HDFS Checkpoint Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's HDFS Checkpoint Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a HDFS Checkpoint Directories Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

secondarynamenode_checkpoint_directories_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

secondarynamenode_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

secondarynamenode_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

secondarynamenode_gc_duration_window

Required

false

SecondaryNameNode Host Health Test

Description

When computing the overall SecondaryNameNode health, consider the host's health.

Related Name

Default Value

true

API Name

secondarynamenode_host_health_enabled

Required

false

SecondaryNameNode Process Health Test

Description

Enables the health test that the SecondaryNameNode's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

secondarynamenode_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

secondarynamenode_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

secondarynamenode_web_metric_collection_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HDFS Checkpoint Directories

Description

Determines where on the local file system the HDFS SecondaryNameNode should store the temporary images to merge. For redundancy, enter a comma-delimited list of directories to replicate the image in all of the directories. Typical values are /data/N/dfs/snn for N = 1, 2, 3...

Related Name

dfs.namenode.checkpoint.dir

Default Value

API Name

fs_checkpoint_dir_list

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

SecondaryNameNode Web UI Port

Description

The SecondaryNameNode HTTP port. If the port is 0, then the server starts on a free port. Combined with the SecondaryNameNode's hostname to build its HTTP address.

Related Name

dfs.namenode.secondary.http-address

Default Value

9868

API Name

dfs_secondary_http_port

Required

false

Secure SecondaryNameNode Web UI Port (TLS/SSL)

Description

The base port where the secure SecondaryNameNode web UI listens.

Related Name

dfs.secondary.https.port

Default Value

9869

API Name

dfs_secondary_https_port

Required

false

Bind SecondaryNameNode to Wildcard Address

Description

If enabled, the SecondaryNameNode binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

secondary_namenode_bind_wildcard

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Java Heap Size of Secondary NameNode in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

secondary_namenode_java_heapsize

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: SecondaryNameNode Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondary_http_port

Required

true

Suppress Parameter Validation: Secure SecondaryNameNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure SecondaryNameNode Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondary_https_port

Required

true

Suppress Parameter Validation: SecondaryNameNode Nameservice

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Nameservice parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondarynamenode_nameservice

Required

true

Suppress Parameter Validation: HDFS Checkpoint Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Checkpoint Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fs_checkpoint_dir_list

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: SecondaryNameNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: SecondaryNameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for Secondary NameNode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Secondary NameNode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_java_opts

Required

true

Suppress Parameter Validation: SecondaryNameNode Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_log_dir

Required

true

Suppress Parameter Validation: SecondaryNameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SecondaryNameNode Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_role_env_safety_valve

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_audit_health

Required

true

Suppress Health Test: HDFS Checkpoint Directories Free Space

Description

Whether to suppress the results of the HDFS Checkpoint Directories Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_checkpoint_directories_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_secondary_name_node_web_metric_collection

Required

true

Service-Wide

Advanced

Legacy Cloudera Manager API Clients Compatibility

Description

Determines how Cloudera Manager will intercept and handle legacy clients trying to read and/or write core parameters. This can be enabled to allow for API clients to continue targeting the HDFS service for reading and/or writing values for these parameters: Cloudera Manager in this case will transparently redirect the read/write operations to the appropriate Core Settings service in the same cluster. Read and Write Compatibility will transparently handle both reading and modifications of parameters.

Related Name

Default Value

read_write

API Name

cm_api_aliasing

Required

false

Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to all roles and client configurations in this HDFS service as well as all its dependent services. Any configs added here will be overridden by their default values in HDFS (which can be found in hdfs-default.xml).

Related Name

Default Value

API Name

core_site_safety_valve

Required

false

Enable HDFS Block Metadata API

Description

Enables DataNode support for the experimental DistributedFileSystem.getFileVBlockStorageLocations API. Applicable to CDH 4.1 and onwards.

Related Name

dfs.datanode.hdfs-blocks-metadata.enabled

Default Value

true

API Name

dfs_datanode_hdfs_blocks_metadata_enabled

Required

false

HDFS Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml

Description

For advanced use only, a string to be inserted into hadoop-policy.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hadoop_policy_config_safety_valve

Required

false

Block Replica Placement Policy

Description

The policy the NameNode will use to place block replicas: The HDFS Default policy places one replica on the node where the client process writing the block resides, one on a randomly-chosen remote rack, and one on a randomly-chosen node in the same remote rack (assuming a replication factor of 3). The Upgrade Domains policy adds an additional layer of grouping based on Upgrade Domain, and must be selected in order to use Upgrade Domains for DataNode hosts.

Related Name

dfs.block.replicator.classname

Default Value

org.apache.hadoop.hdfs.server.blockmanagement.BlockPlacementPolicyDefault

API Name

hdfs_block_placement_policy

Required

true

Shared Hadoop Group Name

Description

The name of the system group shared by all the core Hadoop services.

Related Name

Default Value

hadoop

API Name

hdfs_hadoop_group_name

Required

true

HDFS Replication Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to all HDFS Replication jobs.

Related Name

Default Value

API Name

hdfs_replication_core_site_safety_valve

Required

false

HDFS Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the environment of HDFS replication jobs.

Related Name

Default Value

API Name

hdfs_replication_env_safety_valve

Required

false

HDFS Replication Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only. Key-value pairs (one on each line) to be inserted into the HDFS replication configuration for hadoop-env.sh.

Related Name

Default Value

API Name

hdfs_replication_haoop_env_sh_safety_valve

Required

false

HDFS Replication Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only, a string to be inserted into hdfs-site.xml. Applies to all HDFS Replication jobs.

Related Name

Default Value

API Name

hdfs_replication_hdfs_site_safety_valve

Required

false

HDFS Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only, a string to be inserted into hdfs-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hdfs_service_config_safety_valve

Required

false

HDFS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hdfs_service_env_safety_valve

Required

false

HDFS Snapshot Shell Command Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the environment of HDFS snapshot shell command.

Related Name

Default Value

API Name

hdfs_shell_cmd_env_safety_valve

Required

false

HDFS Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

For advanced use only, a string to be inserted into ssl-server.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hdfs_ssl_server_safety_valve

Required

false

System User's Home Directory

Description

The home directory of the system user on the local filesystem. This setting must reflect the system's configured value - only changing it here will not change the actual home directory.

Related Name

Default Value

/var/lib/hadoop-hdfs

API Name

hdfs_user_home_dir

Required

true

Client Connection Maximum Idle Time

Description

The time after which a client will bring down the connection to the server if idle.

Related Name

ipc.client.connection.maxidletime

Default Value

30 second(s)

API Name

ipc_client_connection_max_idle_time

Required

false

Client Connection Maximum Retries

Description

The number of retries a client will make to establish a server connection.

Related Name

ipc.client.connect.max.retries

Default Value

50

API Name

ipc_client_connection_max_retries

Required

false

Client Idle Threshold

Description

Client connections will be inspected for idleness if the number of connections to the server reaches or exceeds this number.

Related Name

ipc.client.idlethreshold

Default Value

8000

API Name

ipc_client_idle_threshold

Required

false

HDFS Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as (except the HttpFS server, which has its own group)

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as (except the HttpFS server, which has its own user)

Related Name

Default Value

hdfs

API Name

process_username

Required

true

HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-audit.xml

Description

For advanced use only, a string to be inserted into ranger-hdfs-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-hdfs-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml

Description

For advanced use only, a string to be inserted into ranger-hdfs-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for HDFS events:

- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- command: the HDFS operation being performed.
- src: the source path for the operation.
- dest: the destination path for the operation.
- permissions: the permissions associated with the operation.

The default HDFS audit event filter accepts all denied access, delete and rename events, and discards events that affects files in any of the staging directories (Hive, Spark, Impala), events that affect files in /tmp directory, events that affect files in Cloudera Hive Canary directory, events generated by the internal Cloudera and Hadoop users (cloudera-scm, dr.who, hbase, hive, impala, mapred, solr, and spark), and 'ls' actions performed by the hdfs user.

Related Name

navigator.event.filter

Default Value

comment: [The default HDFS audit event filter accepts all denied access, delete , and rename events, and discards events that affects files in any of the , staging directories (Hive, Spark, Impala), events that affect files in /tmp , directory, events that affect files in Cloudera Hive Canary directory, , events generated by the internal Cloudera and Hadoop users (cloudera-scm, , dr.who, hbase, hive, impala, mapred, solr, and spark), and \u0027ls\u0027 actions , performed by the hdfs user.], defaultAction: accept, rules: [action: accept, fields: [name: allowed, match: (?:false)] , action: discard, fields: [name: src, match: (?:.*/\\.hive-staging($|.*)?|.*/\\.staging($|/.*)?|.*/\\.sparkStaging($|/.*)?|.*/_impala_insert_staging($|/.*)?|/user/history/done_intermediate(?:/.*)?|/user/spark/spark2ApplicationHistory($|/.*)|/user/spark/applicationHistory($|/.*)|/user/hue/

\\.cloudera_manager_hive_metastore_canary(?:/.*)?|/user/hue/\\.Trash/Current/user/hue/\\.cloudera_manager_hive_metastore_canary(?:/.*)?|/tmp(?:/.*)?)] , action: accept, fields: [name: operation, match: delete|rename.*] , action: discard, fields: [name: username, match: (?:cloudera-scm|dr.who|hbase|hive|impala|mapred|solr|spark)(?:/.+)?] , action: discard, fields: [name: username, match: (?:hdfs)(?:/.+)? , name: operation, match: (?:listStatus|listCachePools|listCacheDirectives|getfileinfo)] , action: accept, fields: [name: operation, match: (?:getfileinfo)]]

API Name

navigator_audit_event_filter

Required

false

Audit Queue Policy

Description

Action to take when the audit event queue is full. Drop the event or shutdown the affected process.

Related Name

navigator.batch.queue_policy

Default Value

DROP

API Name

navigator_audit_queue_policy

Required

false

Audit Event Tracker

Description

Configures the rules for event tracking and coalescing. This feature is used to define equivalency between different audit events. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the "tracked" events according to the rules defined here. Event trackers are defined in a JSON object like the following: { "timeToLive" : [integer], "fields" : [{ "type" : [string], "name" : [string] }] } Where:

- timeToLive: maximum amount of time an event will be tracked, in milliseconds. Must be provided. This defines how long, since it's first seen, an event will be tracked. A value of 0 disables tracking.
- fields: list of fields to compare when matching events against tracked events.

Each field has an evaluator type associated with it. The evaluator defines how the field data is to be compared. The following evaluators are available:

- value: uses the field value for comparison.
- username: treats the field value as a user name, and ignores any host-specific data. This is useful for environment using Kerberos, so that only the principal name and realm are compared.

The following is the list of fields that can be used to compare HDFS events:

- operation: the HDFS operation being performed.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- src: the source path for the operation.
- dest: the destination path for the operation.

- permissions: the permissions associated with the operation.

The default event tracker for HDFS services defines equality by comparing the username, operation, and source path of the events.

Related Name

navigator_event_tracker

Default Value

comment: [The default event tracker for HDFS services defines equality by , comparing the username, operation, and source path of the events.], timeToLive: 60000, fields: [type: value, name: src , type: value, name: operation , type: username, name: username]

API Name

navigator_event_tracker

Required

false

High Availability

Timeout for Cloudera Manager Fencing Strategy

Description

The timeout, in milliseconds, to use with the Cloudera Manager agent-based fencer.

Related Name

dfs.ha.fencing.cloudera_manager.timeout_millis

Default Value

10000

API Name

dfs_ha_fencing_cloudera_manager_timeout_millis

Required

false

HDFS High Availability Fencing Methods

Description

List of fencing methods to use for service fencing. Setting this to shell(true) enables the built-in HDFS fencing mechanism, which causes the NameNode to exit if it attempts a write operation when it is not active. In almost all cases, this is the best choice. The sshfence method uses SSH. If using custom fencers (that may communicate with shared store, power units, or network switches), use the shell to invoke them.

Related Name

dfs.ha.fencing.methods

Default Value

shell(true)

API Name

dfs_ha_fencing_methods

Required

false

Timeout for SSH Fencing Strategy

Description

SSH connection timeout, in milliseconds, to use with the built-in sshfence fencer.

Related Name

dfs.ha.fencing.ssh.connect-timeout

Default Value

30 second(s)

API Name

dfs_ha_fencing_ssh_connect_timeout

Required

false

Private Keys for SSH Fencing Strategy

Description

The SSH private key files to use with the built-in sshfence fencer. These are to be accessible to the hdfs user on the machines running the NameNodes.

Related Name

dfs.ha.fencing.ssh.private-key-files

Default Value

API Name

dfs_ha_fencing_ssh_private_key_files

Required

false

FailoverProxyProvider Class

Description

Enter a FailoverProxyProvider implementation to configure two URIs to connect to during fail-over. The first configured address is tried first, and on a fail-over event the other address is tried.

Related Name

dfs.client.failover.proxy.provider

Default Value

org.apache.hadoop.hdfs.server.namenode.ha.ConfiguredFailoverProxyProvider

API Name

dfs_ha_proxy_provider

Required

true

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/hadoop-hdfs/audit

API Name

audit_event_log_dir

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Number of Audit Logs to Retain

Description

Maximum number of rolled-over audit logs to retain. The logs are not deleted if they contain audit events that have not yet been propagated to the Audit Server.

Related Name

navigator.client.max_num_audit_log

Default Value

10

API Name

navigator_client_max_num_audit_log

Required

false

Monitoring

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Failover Controllers Healthy

Description

Enables the health check that verifies that the failover controllers associated with this service are healthy and running.

Related Name

Default Value

true

API Name

failover_controllers_healthy_enabled

Required

false

HDFS Health Canary Directory

Description

The service monitor will use this directory to create files to test if the hdfs service is healthy. The directory and files are created with permissions specified by 'HDFS Health Canary Directory Permissions'

Related Name

Default Value

/tmp/.cloudera_health_monitoring_canary_files

API Name

firehose_hdfs_canary_directory

Required

false

HDFS Health Canary Directory Permissions

Description

The service monitor will use these permissions to create the directory and files to test if the hdfs service is healthy. Permissions are specified using the 10-character unix-symbolic format e.g. '-rwxr-xr-x'.

Related Name

Default Value

-rwxrwxrwx

API Name

firehose_hdfs_canary_directory_permissions

Required

false

Active NameNode Detection Window

Description

The tolerance window that will be used in HDFS service tests that depend on detection of the active NameNode.

Related Name

Default Value

3 minute(s)

API Name

hdfs_active_namenode_detection_window

Required

false

Blocks With Corrupt Replicas Monitoring Thresholds

Description

The health check thresholds of the number of blocks that have at least one corrupt replica. Specified as a percentage of the total number of blocks.

Related Name

Default Value

Warning: 0.5 %, Critical: 1.0 %

API Name

hdfs_blocks_with_corrupt_replicas_thresholds

Required

false

HDFS Canary Health Check

Description

Enables the health check that a client can create, read, write, and delete files

Related Name

Default Value

true

API Name

hdfs_canary_health_enabled

Required

false

Healthy DataNode Monitoring Thresholds

Description

The health test thresholds of the overall DataNode health. The check returns "Concerning" health if the percentage of "Healthy" DataNodes falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" DataNodes falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

hdfs_datanodes_healthy_thresholds

Required

false

HDFS Free Space Monitoring Thresholds

Description

The health check thresholds of free space in HDFS. Specified as a percentage of total HDFS capacity.

Related Name

Default Value

Warning: 20.0 %, Critical: 10.0 %

API Name

hdfs_free_space_thresholds

Required

false

Missing Block Monitoring Thresholds

Description

The health check thresholds of the number of missing blocks. Specified as a percentage of the total number of blocks.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

hdfs_missing_blocks_thresholds

Required

false

NameNode Activation Startup Tolerance

Description

The amount of time after NameNode(s) start that the lack of an active NameNode will be tolerated. This is intended to allow either the auto-failover daemon to make a NameNode active, or a

specifically issued failover command to take effect. This is an advanced option that does not often need to be changed.

Related Name

Default Value

3 minute(s)

API Name

hdfs_namenode_activation_startup_tolerance

Required

false

Active NameNode Role Health Check

Description

When computing the overall HDFS cluster health, consider the active NameNode's health

Related Name

Default Value

true

API Name

hdfs_namenode_health_enabled

Required

false

Standby NameNode Health Check

Description

When computing the overall HDFS cluster health, consider the health of the standby NameNode.

Related Name

Default Value

true

API Name

hdfs_standby_namenodes_health_enabled

Required

false

Under-replicated Block Monitoring Thresholds

Description

The health check thresholds of the number of under-replicated blocks. Specified as a percentage of the total number of blocks.

Related Name

Default Value

Warning: 10.0 %, Critical: 40.0 %

API Name

hdfs_under_replicated_blocks_thresholds

Required

false

Erasure Coding Policy Verification Health Check

Description

Enables the health test for verifying if the cluster topology supports all the enabled erasure coding policies.

Related Name

Default Value

false

API Name

hdfs_verify_ec_with_topology_enabled

Required

false

Log Event Retry Frequency

Description

The frequency in which the log4j event publication appender will retry sending undelivered log events to the Event server, in seconds

Related Name

Default Value

30

API Name

log_event_retry_frequency

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>dfs.socket.timeout</name> <value>3000</value> </property> <property> <name>dfs.datanode.socket.write.timeout</name> <value>3000</value> </property> <property> <name>ipc.client.connect.max.retries</name> <value>1</value> </property> <property> <name>fs.permissions.umask-mode</name> <value>000</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Core Settings Connector

Description

Dependency on the Core Settings service for the cluster.

Related Name

Default Value

API Name

core_connector

Required

true

HDFS Block Size

Description

The default block size in bytes for new HDFS files. Note that this value is also used as the HBase Region Server HLog block size.

Related Name

dfs.blocksize

Default Value

128 MiB

API Name

dfs_block_size

Required

false

Check HDFS Permissions

Description

If false, permission checking is turned off for files in HDFS.

Related Name

dfs.permissions

Default Value

true

API Name

dfs_permissions

Required

false

Default Umask

Description

Default umask for file and directory creation, specified in an octal value (with a leading 0)

Related Name

fs.permissions.umask-mode

Default Value

022

API Name

dfs_umaskmode

Required

false

Enable WebHDFS

Description

Enable WebHDFS interface

Related Name

dfs.webhdfs.enabled

Default Value

true

API Name

dfs_webhdfs_enabled

Required

false

Serve logs over HTTP

Description

Whether to serve logs over HTTP from HDFS web servers. This includes listing the logs directory at the /logs endpoint, which may be a security concern.

Related Name

hadoop.http.logs.enabled

Default Value

true

API Name

http_logs_enabled

Required

false

Compression Codecs

Description

Comma-separated list of compression codecs that can be used in job or map compression.

Related Name

io.compression.codecs

Default Value

org.apache.hadoop.io.compress.DefaultCodec org.apache.hadoop.io.compress.GzipCodec org.apache.hadoop.io.compress.BZip2Codec org.apache.hadoop.io.compress.DeflateCodec org.apache.hadoop.io.compress.SnappyCodec org.apache.hadoop.io.compress.Lz4Codec

API Name

io_compression_codecs

Required

false

KMS Service

Description

The Key Management Server used by HDFS. This must be set to use encryption for data at rest.

Related Name

Default Value

API Name

kms_service

Required

false

Ranger Plugin Enable HDFS ACLs Fallback

Description

By default, fallback is enabled for HDFS, which mean if the access cannot be determined by Ranger policies, authorization will fallback to HDFS ACLs. If this behavior needs to be changed, you can disable the config.

Related Name

xasecure.add-hadoop-authorization

Default Value

true

API Name

ranger_plugin_enable_fallback_authorization

Required

false

Ranger Service Name

Description

Name of the Ranger service/repository where service related data will be stored

Related Name

ranger.plugin.hdfs.service.name

Default Value

GENERATED_RANGER_SERVICE_NAME

API Name

ranger_plugin_service_name

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hdfs.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hdfs.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this HDFS service instance depends on. This config is used for enabling Ranger authorization in the HDFS instance not used by Ranger.

Related Name

Default Value

API Name

ranger_service

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this HDFS service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Performance

DataNode Local Path Access Users

Description

Comma separated list of users allowed to do short circuit read. A short circuit read allows a client co-located with the data to read HDFS file blocks directly from HDFS. If empty, will default to the DataNode process' user.

Related Name

dfs.block.local-path-access.user

Default Value

API Name

dfs_block_local_path_access_user

Required

false

HDFS File Block Storage Location Timeout

Description

Timeout in milliseconds for the parallel RPCs made in DistributedFileSystem#getFileBlockStorageLocations(). This value is only emitted for Impala.

Related Name

dfs.client.file-block-storage-locations.timeout.millis

Default Value

10 second(s)

API Name

dfs_client_file_block_storage_locations_timeout

Required

false

Enable HDFS Short-Circuit Read

Description

Enable HDFS short-circuit read. This allows a client colocated with the DataNode to read HDFS file blocks directly. This gives a performance boost to distributed clients that are aware of locality.

Related Name

dfs.client.read.shortcircuit

Default Value

true

API Name

dfs_datanode_read_shortcircuit

Required

false

UNIX Domain Socket path

Description

Path on the DataNode's local file system to a UNIX domain socket used for communication between the DataNode and local HDFS clients. This socket is used for Short Circuit Reads. Only the HDFS System User and "root" should have write access to the parent directory and all of its ancestors. This property is supported in CDH 4.2 or later deployments.

Related Name

dfs.domain.socket.path

Default Value

/var/run/hdfs-sockets/dn

API Name

dfs_domain_socket_path

Required

false

FsImage Transfer Bandwidth

Description

Maximum bandwidth used for image transfer in bytes per second. This can help keep normal NameNode operations responsive during checkpointing. A default value of 0 indicates that throttling is disabled.

Related Name

dfs.image.transfer.bandwidthPerSec

Default Value

0 B

API Name

dfs_image_transfer_bandwidthPerSec

Required

false

FsImage Transfer Socket Timeout

Description

Socket timeout for the HttpURLConnection instance used in the image transfer. This is measured in milliseconds. This timeout prevents client hangs if the connection is idle for this configured timeout, during image transfer.

Related Name

dfs.image.transfer.timeout

Default Value

1 minute(s)

API Name

dfs_image_transfer_timeout

Required

false

Access Time Precision

Description

Precision of access time for HDFS files. Setting it to 0 disables access times for HDFS.

Related Name

dfs.namenode.accesstime.precision

Default Value

0 second(s)

API Name

dfs_namenode_accesstime_precision

Required

false

NameNode Startup Block Deletion Delay

Description

Block deletion in NameNode is paused for this period of time after startup. The suggested delay is 1 hour to give the administrator enough time to notice a large number of blocks pending deletion and take corrective action.

Related Name

dfs.namenode.startup.delay.block.deletion.sec

Default Value

1 hour(s)

API Name

dfs_namenode_startup_delay_block_deletion_sec

Required

false

Ports and Addresses

Use DataNode Hostname

Description

Typically, HDFS clients and servers communicate by opening sockets via an IP address. In certain networking configurations, it is preferable to open sockets after doing a DNS lookup on the hostname. Enable this property to open sockets after doing a DNS lookup on the hostname. This property is supported in CDH3u4 or later deployments.

Related Name

dfs.client.use.datanode.hostname

Default Value

false

API Name

dfs_client_use_datanode_hostname

Required

false

Replication

Maintenance State Minimal Block Replication

Description

The minimum number of block replicas required to enter Maintenance State. If any block has less than the minimum number of block replicas, the DataNode cannot immediately enter Maintenance State.

Related Name

dfs.namenode.maintenance.replication.min

Default Value

1

API Name

dfs_maintenance_replication_min

Required

false

Replication Factor

Description

Default block replication. The number of replications to make when the file is created. The default value is used if a replication number is not specified.

Related Name

dfs.replication

Default Value

3

API Name

dfs_replication

Required

false

Maximal Block Replication

Description

The maximal block replication.

Related Name

dfs.replication.max

Default Value

512

API Name

dfs_replication_max

Required

false

Minimal Block Replication

Description

The minimal block replication.

Related Name

dfs.namenode.replication.min

Default Value

1

API Name

dfs_replication_min

Required

false

Security

DataNode Data Transfer Protection

Description

SASL protection mode for secured connections to the DataNodes when reading or writing data. Value is the type of SASL protection to be used for secured connections to the DataNode when reading or writing block data. Possible values are 'authentication', 'integrity' and 'privacy'. authentication means authentication only and no integrity or privacy; integrity implies that only authentication and integrity are enabled; and privacy implies all of authentication, integrity and privacy are enabled. If "Enable Data Transfer Encryption" is set to true, then it supersedes the setting for this parameter and enforces that all connections must use a specialized encrypted SASL handshake. This property is ignored for connections to a DataNode listening on a privileged port. In this case, it is assumed that the use of a privileged port establishes sufficient trust.

Related Name

dfs.data.transfer.protection

Default Value

API Name

dfs_data_transfer_protection

Required

false

Enable Data Transfer Encryption

Description

Enable encryption of data transfer between DataNodes and clients, and among DataNodes. When enabled, block data that is read/written from/to HDFS will be encrypted on the wire. For effective data transfer protection, enable Kerberos authentication and pick privacy for "Hadoop RPC Protection".

Related Name

dfs.encrypt.data.transfer

Default Value

false

API Name

dfs_encrypt_data_transfer

Required

false

Data Transfer Encryption Algorithm

Description

Algorithm to encrypt data transfer between DataNodes and clients, and among DataNodes. If 3des or rc4 are chosen, the entire communication is encrypted with that algorithm. In CDH 5.4 and higher, if AES/CTR/NoPadding is chosen, 3des is used for the initial key exchange, and then AES/CTR/NoPadding is used for the transfer of data. This is the most secure option, and is recommended for clusters running CDH 5.4 or higher. It also requires that the "openssl-devel" package be installed on all machines in the cluster. When this parameter is changed, a full, nonrolling restart of the cluster must be performed.

Related Name

dfs.encrypt.data.transfer.algorithm

Default Value

rc4

API Name

dfs_encrypt_data_transfer_algorithm

Required

false

Data Transfer Cipher Suite Key Strength

Description

If AES/CTR/NoPadding is chosen for the Data Transfer Encryption Algorithm, this specifies the length (in bits) of the AES key. When this parameter is changed, a full, non-rolling restart of the cluster must be performed.

Related Name

dfs.encrypt.data.transfer.cipher.key.bitlength

Default Value

256

API Name

dfs_encrypt_data_transfer_cipher_keybits

Required

false

Enable Access Control Lists

Description

ACLs (Access Control Lists) enhance the existing HDFS permission model to support controlling file access for arbitrary combinations of users and groups instead of a single owner, single group, and all other users. When ACLs are disabled, the NameNode rejects all attempts to set an ACL.

Related Name

dfs.namenode.acls.enabled

Default Value

true

API Name

dfs_namenode_acls_enabled

Required

false

Superuser Group

Description

The name of the group of superusers.

Related Name

dfs.permissions.superusergroup

Default Value

supergroup

API Name

dfs_permissions_supergroup

Required

false

Enable Ranger Authorization

Description

Enable fine-grained security using Ranger. There should be only one Ranger service installed in the same cluster as HDFS: this Ranger service should have the DFS dependency set to this HDFS service.

Related Name

Default Value

false

API Name

enable_ranger_authorization

Required

false

Enable Kerberos Authentication for HTTP Web-Consoles

Description

Enables Kerberos authentication for Hadoop HTTP web consoles for all roles of this service using the SPNEGO protocol. Note: This is effective only if Kerberos is enabled.

Related Name

Default Value

false

API Name

hadoop_secure_web_ui

Required

false

HDFS User to Impersonate

Description

The user the management services impersonates when connecting to HDFS. If no value is specified, the HDFS superuser is used.

Related Name

Default Value

API Name

hdfs_user_to_impersonate

Required

false

Hue's Kerberos Principal Short Name

Description

The short name of the Hue Kerberos principal. Normally, you do not need to specify this configuration. Cloudera Manager auto-configures this property so that Hue and Cloudera Manamgent Service work properly.

Related Name

hue.kerberos.principal.shortname

Default Value

API Name

hue_kerberos_principal_shortname

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hdfs

API Name

kerberos_princ_name

Required

true

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hdfs

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hdfs/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hdfs/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hdfs.policy.cache.dir

Default Value

/var/lib/ranger/hdfs/policy-cache

API Name

ranger_policy_cache_dir

Required

false

Hadoop TLS/SSL Server Keystore Key Password

Description

Password that protects the private key contained in the server keystore used for encrypted shuffle and encrypted web UIs. Applies to all configurations of daemon roles of this service.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Hadoop TLS/SSL Server Keystore File Location

Description

Path to the keystore file containing the server certificate and private key used for encrypted shuffle and encrypted web UIs. Applies to configurations of all daemon roles of this service.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Hadoop TLS/SSL Server Keystore File Password

Description

Password for the server keystore file used for encrypted shuffle and encrypted web UIs. Applies to configurations of all daemon roles of this service.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

SSL/TLS Cipher Suite

Description

The SSL/TLS cipher suites to use. "Modern 2018" is a modern set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. These cipher suites use strong cryptography and are preferred unless interaction with older clients is required. These modern cipher suites are compatible with Firefox 27, Chrome 22, Internet Explorer 11, Opera 14, Safari 7, Android 4.4, and Java 8. "Intermediate 2018" is an intermediate set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. Select the Intermediate 2018 cipher suites if you require compatibility with a wider range of clients, legacy browsers, or older Linux tools.

Related Name

ssl.server.exclude.cipher.list

Default Value

modern2018

API Name

tls_ciphers

Required

false

Suppressions

Suppress Configuration Validator: Balancer Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the Balancer Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_config_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for Balancer

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_java_opts

Required

true

Suppress Configuration Validator: Balancer Log Directory

Description

Whether to suppress configuration warnings produced by the Balancer Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_balancer_log_dir

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: DataNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the DataNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_config_safety_valve

Required

true

Suppress Configuration Validator: DataNode Failed Volumes Tolerated Validator

Description

Whether to suppress configuration warnings produced by the DataNode Failed Volumes Tolerated Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_failed_volumes_validator

Required

true

Suppress Configuration Validator: Java Heap Size of DataNode in Bytes

Description

Whether to suppress configuration warnings produced by the Java Heap Size of DataNode in Bytes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_java_heapsize

Required

true

Suppress Configuration Validator: Java Configuration Options for DataNode

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for DataNode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_java_opts

Required

true

Suppress Configuration Validator: DataNode Log Directory

Description

Whether to suppress configuration warnings produced by the DataNode Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_log_dir

Required

true

Suppress Configuration Validator: DataNode Reserved Space Validator

Description

Whether to suppress configuration warnings produced by the DataNode Reserved Space Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_reserved_space_validator

Required

true

Suppress Configuration Validator: DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the DataNode Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datanode_role_env_safety_valve

Required

true

Suppress Configuration Validator: DataNode Data Directory

Description

Whether to suppress configuration warnings produced by the DataNode Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_data_dir_list

Required

true

Suppress Configuration Validator: DataNode Data Directory Permissions

Description

Whether to suppress configuration warnings produced by the DataNode Data Directory Permissions configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_data_dir_perm

Required

true

Suppress Configuration Validator: DataNode HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the DataNode HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_http_port

Required

true

Suppress Configuration Validator: Secure DataNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure DataNode Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_https_port

Required

true

Suppress Configuration Validator: DataNode Protocol Port

Description

Whether to suppress configuration warnings produced by the DataNode Protocol Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_ipc_port

Required

true

Suppress Configuration Validator: DataNode Transceiver Port

Description

Whether to suppress configuration warnings produced by the DataNode Transceiver Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_datanode_port

Required

true

Suppress Configuration Validator: NameNode Nameservice

Description

Whether to suppress configuration warnings produced by the NameNode Nameservice configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_federation_namenode_nameservice

Required

true

Suppress Configuration Validator: NameNode Web UI Port

Description

Whether to suppress configuration warnings produced by the NameNode Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_http_port

Required

true

Suppress Configuration Validator: Secure NameNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure NameNode Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_https_port

Required

true

Suppress Configuration Validator: JournalNode Edits Directory

Description

Whether to suppress configuration warnings produced by the JournalNode Edits Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_edits_dir

Required

true

Suppress Configuration Validator: JournalNode HTTP Port

Description

Whether to suppress configuration warnings produced by the JournalNode HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_http_port

Required

true

Suppress Configuration Validator: Secure JournalNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure JournalNode Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_https_port

Required

true

Suppress Configuration Validator: JournalNode RPC Port

Description

Whether to suppress configuration warnings produced by the JournalNode RPC Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_journalnode_rpc_port

Required

true

Suppress Configuration Validator: NameNode Data Directories

Description

Whether to suppress configuration warnings produced by the NameNode Data Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_name_dir_list

Required

true

Suppress Configuration Validator: NameNode Edits Directories

Description

Whether to suppress configuration warnings produced by the NameNode Edits Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_edits_dir

Required

true

Suppress Configuration Validator: NameNode Handler Count Minimum Validator

Description

Whether to suppress configuration warnings produced by the NameNode Handler Count Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_handler_count_minimum_validator

Required

true

Suppress Configuration Validator: Quorum-based Storage Journal name

Description

Whether to suppress configuration warnings produced by the Quorum-based Storage Journal name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_quorum_journal_name

Required

true

Suppress Configuration Validator: NameNode Service Handler Count Minimum Validator

Description

Whether to suppress configuration warnings produced by the NameNode Service Handler Count Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_service_handler_count_minimum_validator

Required

true

Suppress Configuration Validator: NameNode Service RPC Port

Description

Whether to suppress configuration warnings produced by the NameNode Service RPC Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_servicerpc_address

Required

true

Suppress Configuration Validator: Shared Edits Directory

Description

Whether to suppress configuration warnings produced by the Shared Edits Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_namenode_shared_edits_dir

Required

true

Suppress Configuration Validator: Temporary Dump Directory

Description

Whether to suppress configuration warnings produced by the Temporary Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_nfs3_dump_dir

Required

true

Suppress Configuration Validator: Allowed Hosts and Privileges

Description

Whether to suppress configuration warnings produced by the Allowed Hosts and Privileges configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_nfs_exports_allowed_hosts

Required

true

Suppress Configuration Validator: SecondaryNameNode Web UI Port

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondary_http_port

Required

true

Suppress Configuration Validator: Secure SecondaryNameNode Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure SecondaryNameNode Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondary_https_port

Required

true

Suppress Configuration Validator: SecondaryNameNode Nameservice

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Nameservice configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs_secondarynamenode_nameservice

Required

true

Suppress Configuration Validator: Java Configuration Options for Failover Controller

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Failover Controller configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_failover_controller_java_opts

Required

true

Suppress Configuration Validator: Failover Controller Log Directory

Description

Whether to suppress configuration warnings produced by the Failover Controller Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_failover_controller_log_dir

Required

true

Suppress Configuration Validator: Failover Controller Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Failover Controller Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_failovercontroller_role_env_safety_valve

Required

true

Suppress Configuration Validator: Failover Controller Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the Failover Controller Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fc_config_safety_valve

Required

true

Suppress Configuration Validator: HDFS Checkpoint Directories

Description

Whether to suppress configuration warnings produced by the HDFS Checkpoint Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fs_checkpoint_dir_list

Required

true

Suppress Configuration Validator: Filesystem Trash Interval On Validator

Description

Whether to suppress configuration warnings produced by the Filesystem Trash Interval On Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fs_trash_interval_minimum_validator

Required

true

Suppress Configuration Validator: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Configuration Validator: HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_config_safety_valve

Required

true

Suppress Configuration Validator: HDFS Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the HDFS Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_client_java_opts

Required

true

Suppress Configuration Validator: Administration Port

Description

Whether to suppress configuration warnings produced by the Administration Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_admin_port

Required

true

Suppress Configuration Validator: REST Port

Description

Whether to suppress configuration warnings produced by the REST Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_http_port

Required

true

Suppress Configuration Validator: Signature Secret

Description

Whether to suppress configuration warnings produced by the Signature Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_httpfs_signature_secret

Required

true

Suppress Configuration Validator: HDFS Trash Enabled Validator

Description

Whether to suppress configuration warnings produced by the HDFS Trash Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdfs_trash_disabled_validator

Required

true

Suppress Configuration Validator: HttpFS Advanced Configuration Snippet (Safety Valve) for httpfs-site.xml

Description

Whether to suppress configuration warnings produced by the HttpFS Advanced Configuration Snippet (Safety Valve) for httpfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_config_safety_valve

Required

true

Suppress Configuration Validator: HttpFS Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the HttpFS Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_core_site_safety_valve

Required

true

Suppress Configuration Validator: HttpFS Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the HttpFS Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_hdfs_site_safety_valve

Required

true

Suppress Configuration Validator: HttpFS TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HttpFS TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_keystore_file

Required

true

Suppress Configuration Validator: HttpFS TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HttpFS TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_keystore_password

Required

true

Suppress Configuration Validator: HttpFS TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the HttpFS TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_truststore_file

Required

true

Suppress Configuration Validator: HttpFS TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the HttpFS TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_https_truststore_password

Required

true

Suppress Configuration Validator: Java Configuration Options for HttpFS

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HttpFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_java_opts

Required

true

Suppress Configuration Validator: HttpFS Load Balancer

Description

Whether to suppress configuration warnings produced by the HttpFS Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_load_balancer

Required

true

Suppress Configuration Validator: HttpFS Log Directory

Description

Whether to suppress configuration warnings produced by the HttpFS Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_log_dir

Required

true

Suppress Configuration Validator: System Group

Description

Whether to suppress configuration warnings produced by the System Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_process_groupname

Required

true

Suppress Configuration Validator: System User

Description

Whether to suppress configuration warnings produced by the System User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_process_username

Required

true

Suppress Configuration Validator: HttpFS Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HttpFS Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: JournalNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the JournalNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jn_config_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for JournalNode

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for JournalNode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_java_opts

Required

true

Suppress Configuration Validator: JournalNode Log Directory

Description

Whether to suppress configuration warnings produced by the JournalNode Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_log_dir

Required

true

Suppress Configuration Validator: JournalNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the JournalNode Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_journalnode_role_env_safety_valve

Required

true

Suppress Configuration Validator: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the Role-Specific Kerberos Principal configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Configuration Validator: DataNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the DataNode Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the Rules to Extract Events from Log Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Configuration Validator: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_all_hosts.txt

Description

Whether to suppress configuration warnings produced by the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_all_hosts.txt configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_all_hosts_safety_valve

Required

true

Suppress Configuration Validator: NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_config_safety_valve

Required

true

Suppress Configuration Validator: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_allow.txt

Description

Whether to suppress configuration warnings produced by the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_allow.txt configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_hosts_allow_safety_valve

Required

true

Suppress Configuration Validator: NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_exclude.txt

Description

Whether to suppress configuration warnings produced by the NameNode Advanced Configuration Snippet (Safety Valve) for dfs_hosts_exclude.txt configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_hosts_exclude_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of NameNode in Bytes Minimum Validator

Description

Whether to suppress configuration warnings produced by the Java Heap Size of NameNode in Bytes Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_java_heapsize_minimum_validator

Required

true

Suppress Configuration Validator: Java Configuration Options for NameNode

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for NameNode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_java_opts

Required

true

Suppress Configuration Validator: NameNode Log Directory

Description

Whether to suppress configuration warnings produced by the NameNode Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_log_dir

Required

true

Suppress Configuration Validator: NameNode Port

Description

Whether to suppress configuration warnings produced by the NameNode Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_port

Required

true

Suppress Configuration Validator: NameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the NameNode Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_role_env_safety_valve

Required

true

Suppress Configuration Validator: HDFS NameNode TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the HDFS NameNode TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_truststore_file

Required

true

Suppress Configuration Validator: HDFS NameNode TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the HDFS NameNode TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_namenode_truststore_password

Required

true

Suppress Configuration Validator: Validates Nameservices do not conflict between base and compute clusters.

Description

Whether to suppress configuration warnings produced by the Validates Nameservices do not conflict between base and compute clusters. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nameservice_conflict_validator

Required

true

Suppress Configuration Validator: Mount Points

Description

Whether to suppress configuration warnings produced by the Mount Points configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nameservice_mountpoints

Required

true

Suppress Configuration Validator: NFS Gateway Web UI Port

Description

Whether to suppress configuration warnings produced by the NFS Gateway Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_http_port

Required

true

Suppress Configuration Validator: Secure NFS Gateway Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure NFS Gateway Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_https_port

Required

true

Suppress Configuration Validator: NFS Gateway MountD Port

Description

Whether to suppress configuration warnings produced by the NFS Gateway MountD Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_mountd_port

Required

true

Suppress Configuration Validator: Portmap (or Rpcbind) Port

Description

Whether to suppress configuration warnings produced by the Portmap (or Rpcbind) Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_portmap_port

Required

true

Suppress Configuration Validator: NFS Gateway Server Port

Description

Whether to suppress configuration warnings produced by the NFS Gateway Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs3_server_port

Required

true

Suppress Configuration Validator: NFS Gateway Export Point

Description

Whether to suppress configuration warnings produced by the NFS Gateway Export Point configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfs_export_point

Required

true

Suppress Configuration Validator: NFS Gateway Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the NFS Gateway Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_config_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for NFS Gateway

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for NFS Gateway configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_java_opts

Required

true

Suppress Configuration Validator: NFS Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the NFS Gateway Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_log_dir

Required

true

Suppress Configuration Validator: NFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the NFS Gateway Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nfsgateway_role_env_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml

Description

Whether to suppress configuration warnings produced by the NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_security_role_safety_valve

Required

true

Suppress Configuration Validator: Excluded Hosts

Description

Whether to suppress configuration warnings produced by the Excluded Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_exclude_hosts

Required

true

Suppress Configuration Validator: Included Hosts

Description

Whether to suppress configuration warnings produced by the Included Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_include_hosts

Required

true

Suppress Configuration Validator: Source Hosts

Description

Whether to suppress configuration warnings produced by the Source Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rebalancer_source_hosts

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: SecondaryNameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_config_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for Secondary NameNode

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Secondary NameNode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_java_opts

Required

true

Suppress Configuration Validator: SecondaryNameNode Log Directory

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_log_dir

Required

true

Suppress Configuration Validator: SecondaryNameNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secondarynamenode_role_env_safety_valve

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Topology Script File Name

Description

Whether to suppress configuration warnings produced by the Topology Script File Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_topology_script_file_name

Required

true

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Auto Failover Validator

Description

Whether to suppress configuration warnings produced by the Auto Failover Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_auto_failover_validator

Required

true

Suppress Configuration Validator: Balancer Count Validator

Description

Whether to suppress configuration warnings produced by the Balancer Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_balancer_count_validator

Required

true

Suppress Parameter Validation: Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_core_site_safety_valve

Required

true

Suppress Configuration Validator: DataNode Count Validator

Description

Whether to suppress configuration warnings produced by the DataNode Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_datanode_count_validator

Required

true

Suppress Parameter Validation: DataNode Local Path Access Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DataNode Local Path Access Users parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_block_local_path_access_user

Required

true

Suppress Parameter Validation: UNIX Domain Socket path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the UNIX Domain Socket path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_domain_socket_path

Required

true

Suppress Parameter Validation: HDFS High Availability Fencing Methods

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS High Availability Fencing Methods parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_ha_fencing_methods

Required

true

Suppress Parameter Validation: Private Keys for SSH Fencing Strategy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Private Keys for SSH Fencing Strategy parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_ha_fencing_ssh_private_key_files

Required

true

Suppress Parameter Validation: FailoverProxyProvider Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the FailoverProxyProvider Class parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_ha_proxy_provider

Required

true

Suppress Parameter Validation: Superuser Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Superuser Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_permissions_supergroup

Required

true

Suppress Parameter Validation: Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replication Factor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_dfs_replication

Required

true

Suppress Configuration Validator: Failover Controller Count Validator

Description

Whether to suppress configuration warnings produced by the Failover Controller Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_failovercontroller_count_validator

Required

true

Suppress Parameter Validation: HDFS Health Canary Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Health Canary Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_firehose_hdfs_canary_directory

Required

true

Suppress Parameter Validation: HDFS Health Canary Directory Permissions

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Health Canary Directory Permissions parameter.

Related Name

Default Value

false

API Name

service_config_suppression_firehose_hdfs_canary_directory_permissions

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_policy_config_safety_valve

Required

true

Suppress Configuration Validator: Secure Web UI Validator

Description

Whether to suppress configuration warnings produced by the Secure Web UI Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_secure_web_ui

Required

true

Suppress Configuration Validator: Hadoop TLS/SSL Validator

Description

Whether to suppress configuration warnings produced by the Hadoop TLS/SSL Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_ssl_validator

Required

true

Suppress Configuration Validator: Data Transfer Encryption Algorithm Validator

Description

Whether to suppress configuration warnings produced by the Data Transfer Encryption Algorithm Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_encrypt_data_transfer_algorithm_validator

Required

true

Suppress Configuration Validator: HDFS Encryption Validator

Description

Whether to suppress configuration warnings produced by the HDFS Encryption Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_encryption_validator

Required

true

Suppress Parameter Validation: Shared Hadoop Group Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Shared Hadoop Group Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_hadoop_group_name

Required

true

Suppress Configuration Validator: Check HDFS Permissions Validator

Description

Whether to suppress configuration warnings produced by the Check HDFS Permissions Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_permissions_validator

Required

true

Suppress Parameter Validation: HDFS Replication Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_replication_core_site_safety_valve

Required

true

Suppress Parameter Validation: HDFS Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_replication_env_safety_valve

Required

true

Suppress Parameter Validation: HDFS Replication Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_replication_haoop_env_sh_safety_valve

Required

true

Suppress Parameter Validation: HDFS Replication Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_replication_hdfs_site_safety_valve

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_service_config_safety_valve

Required

true

Suppress Parameter Validation: HDFS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_service_env_safety_valve

Required

true

Suppress Parameter Validation: HDFS Snapshot Shell Command Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Snapshot Shell Command Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_shell_cmd_env_safety_valve

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_ssl_server_safety_valve

Required

true

Suppress Configuration Validator: HDFS Unassigned Upgrade Domains Validator

Description

Whether to suppress configuration warnings produced by the HDFS Unassigned Upgrade Domains Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_upgrade_domains_unassigned_validator

Required

true

Suppress Configuration Validator: HDFS Unique Upgrade Domains Validator

Description

Whether to suppress configuration warnings produced by the HDFS Unique Upgrade Domains Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_upgrade_domains_unique_validator

Required

true

Suppress Parameter Validation: System User's Home Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User's Home Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_user_home_dir

Required

true

Suppress Parameter Validation: HDFS User to Impersonate

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS User to Impersonate parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_user_to_impersonate

Required

true

Suppress Configuration Validator: HttpFS Count Validator

Description

Whether to suppress configuration warnings produced by the HttpFS Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_httpfs_count_validator

Required

true

Suppress Parameter Validation: Hue's Kerberos Principal Short Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue's Kerberos Principal Short Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_kerberos_principal_shortname

Required

true

Suppress Parameter Validation: Compression Codecs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Compression Codecs parameter.

Related Name

Default Value

false

API Name

service_config_suppression_io_compression_codecs

Required

true

Suppress Configuration Validator: JournalNode Count Validator

Description

Whether to suppress configuration warnings produced by the JournalNode Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_journalnode_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: NameNode Count Validator

Description

Whether to suppress configuration warnings produced by the NameNode Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_namenode_count_validator

Required

true

Suppress Configuration Validator: Nameservice Checkpoint Configuration Validator

Description

Whether to suppress configuration warnings produced by the Nameservice Checkpoint Configuration Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nameservice_checkpoint_configuration_validator

Required

true

Suppress Configuration Validator: Nameservice Mountpoints Validator

Description

Whether to suppress configuration warnings produced by the Nameservice Mountpoints Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nameservice_mountpoints_validator

Required

true

Suppress Configuration Validator: Nameservice Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Nameservice Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nameservice_namenodes_heap_size_validator

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: HDFS Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Audit Event Tracker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Tracker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_event_tracker

Required

true

Suppress Configuration Validator: NFS High Availability Validator

Description

Whether to suppress configuration warnings produced by the NFS High Availability Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nfs_ha_validator

Required

true

Suppress Configuration Validator: NFS Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the NFS Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nfsgateway_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Service Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_service_name

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Configuration Validator: SecondaryNameNode Count Validator

Description

Whether to suppress configuration warnings produced by the SecondaryNameNode Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_secondarynamenode_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Configuration Validator: Short-Circuit Read Enabled Validator

Description

Whether to suppress configuration warnings produced by the Short-Circuit Read Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_short_circuit_read_validator

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_password

Required

true

Suppress Health Test: Corrupt Blocks

Description

Whether to suppress the results of the Corrupt Blocks heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_blocks_with_corrupt_replicas

Required

true

Suppress Health Test: HDFS Canary

Description

Whether to suppress the results of the HDFS Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_canary_health

Required

true

Suppress Health Test: DataNode Health

Description

Whether to suppress the results of the DataNode Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_data_nodes_healthy

Required

true

Suppress Health Test: Failover Controllers Health

Description

Whether to suppress the results of the Failover Controllers Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_failover_controllers_healthy

Required

true

Suppress Health Test: Free Space

Description

Whether to suppress the results of the Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_free_space_remaining

Required

true

Suppress Health Test: NameNode Health

Description

Whether to suppress the results of the NameNode Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_ha_namenode_health

Required

true

Suppress Health Test: Missing Blocks

Description

Whether to suppress the results of the Missing Blocks heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_missing_blocks

Required

true

Suppress Health Test: Under-Replicated Blocks

Description

Whether to suppress the results of the Under-Replicated Blocks heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_under_replicated_blocks

Required

true

Suppress Health Test: Erasure Coding Policy Verification Test

Description

Whether to suppress the results of the Erasure Coding Policy Verification Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hdfs_verify_ec_with_topology

Required

true

Hive Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hive

API Name

client_config_root_dir

Required

true

Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for hive-site.xml.

Related Name

Default Value

API Name

hive_client_config_safety_valve

Required

false

Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hive-env.sh

Related Name

Default Value

API Name

hive_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

hive_client_java_opts

Required

false

Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server. Consider increasing this if you have tables with a lot of metadata and see timeout errors. Used by most Hive Metastore clients such as Hive CLI and HiveServer2, but not by Impala. Impala has a separately configured timeout.

Related Name

hive.metastore.client.socket.timeout

Default Value

5 minute(s)

API Name

hive_metastore_timeout

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

2 GiB

API Name

hive_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Hive Metastore Server

Advanced

Turn on compactor initiator thread.

Description

When enabled, the initiator and cleaner threads will run on this Hive Metastore instance.

Related Name

hive.compactor.initiator.on

Default Value

true

API Name

hive_compactor_initiator_on

Required

true

Number of Threads Used by Compactor

Description

Number of compactor worker threads to run on this metastore instance. Can be different values on different Metastore instances.

Related Name

hive.compactor.worker.threads

Default Value

5

API Name

hive_compactor_worker_threads

Required

true

Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hive_metastore_config_safety_valve

Required

false

Hive Metastore Delegation Token Store

Description

The delegation token store implementation class. Use DBTokenStore for Highly Available Metastore Configuration.

Related Name

hive.cluster.delegation.token.store.class

Default Value

org.apache.hadoop.hive.thrift.MemoryTokenStore

API Name

hive_metastore_delegation_token_store

Required

false

Hive Metastore Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

hive_metastore_env_safety_valve

Required

false

Turn on Hive Metastore housekeeping threads.

Description

When enabled, the threads listed under metastore.task.threads.remote (defaults: AcidHouseKeeperService, AcidOpenTxnsCounterService, AcidCompactionHistoryService, AcidWriteSetService, MaterializationsRebuildLockCleanerTask, PartitionManagementTask) will be started when the Hive Metastore is started.

Related Name

hive.metastore.housekeeping.threads.on

Default Value

true

API Name

hive_metastore_housekeeping_threads_on

Required

true

Java Configuration Options for Hive Metastore Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hive_metastore_java_opts

Required

false

Max Hive Metastore Server Threads

Description

Maximum number of worker threads in the Hive Metastore Server's thread pool

Related Name

hive.metastore.server.max.threads

Default Value

100000

API Name

hive_metastore_max_threads

Required

true

Min Hive Metastore Server Threads

Description

Minimum number of worker threads in the Hive Metastore Server's thread pool

Related Name

hive.metastore.server.min.threads

Default Value

200

API Name

hive_metastore_min_threads

Required

true

Run compactor on Hive Metastore or HiveServer2.

Description

Choose where the compactor worker threads should run. Only possible values are metastore or hs2.

Related Name

hive.metastore.runworker.in

Default Value

hs2

API Name

hive_metastore_runworker_in

Required

true

Max Message Size for Hive MetaStore

Description

Maximum message size Hive MetaStore accepts.

Related Name

hive.metastore.server.max.message.size

Default Value

100 MiB

API Name

hive_metastore_server_max_message_size

Required

false

Enable Metrics Subsystem

Description

Controls whether the Hive metrics subsystem is enabled for the role.

Related Name

hive.metastore.metrics.enabled

Default Value

true

API Name

hive_metrics_enabled

Required

false

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hive/metrics-hivemetastore/metrics.log. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.location

Default Value

API Name

hive_metrics_sample_file_location

Required

false

Metrics Sample File Logging Frequency

Description

The frequency at which the metrics are logged to the sample file. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.frequency

Default Value

30 second(s)

API Name

hive_metrics_sample_logging_frequency

Required

false

Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

hms_core_site_safety_valve

Required

false

Hive Metastore Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Hive Metastore Server Log Directory

Description

Directory where Hive Metastore Server will place its log files.

Related Name

Default Value

/var/log/hive

API Name

hive_log_dir

Required

false

Enable Performance Logging

Description

When enabled, it captures time spent during each part of the query execution for the role.

Related Name

hive.metastore.performance.logging.enabled

Default Value

true

API Name

hive_performance_logging_enabled

Required

false

Hive Metastore Server Logging Threshold

Description

The minimum log level for Hive Metastore Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Hive Metastore Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Hive Metastore Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Hive Metastore Server Max Log Size

Description

The maximum size, in megabytes, per log file for Hive Metastore Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hivemetastore_fd_thresholds

Required

false

Hive Metastore Server Host Health Test

Description

When computing the overall Hive Metastore Server health, consider the host's health.

Related Name

Default Value

true

API Name

hivemetastore_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

hivemetastore_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

hivemetastore_pause_duration_window

Required

false

Hive Metastore Server Process Health Test

Description

Enables the health test that the Hive Metastore Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hivemetastore_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11120

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'metrics<name=(jvm\.pause.*)><>(.*): (\d+)' name: $1_$2 value: $3

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Hive Metastore Canary Health Test

Description

Enables the health test that checks that basic Hive Metastore operations succeed

Related Name

Default Value

true

API Name

metastore_canary_health_enabled

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: strict metric_names: #memory - jvm_buffer_pool_used_bytes - jvm_buffer_pool_capacity_bytes - jvm_buffer_pool_used_buffers - jvm_memory_bytes_used - jvm_memory_bytes_committed - jvm_memory_bytes_max - jvm_memory_bytes_init #gc - jvm_gc_collection_seconds #threads - jvm_threads_current - jvm_threads_daemon - jvm_threads_peak - jvm_threads_started_total - jvm_threads_deadlocked - jvm_threads_deadlocked_monitor - jvm_threads_state #classes - jvm_classes_currently_loaded #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes - jvm_pause_extrasleeptime_count

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id:

$CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Stored Notifications in Database

Description

Enable stored notifications of metadata changes. When enabled, each metadata change will be stored in NOTIFICATION_LOG.

Related Name

Default Value

true

API Name

hive_enable_db_notification

Required

false

Enable Readonly mode for databases

Description

Registers Pre-execution hook which makes database readonly.

Related Name

Default Value

false

API Name

hive_enforce_read_only

Required

false

Time-to-live for Database Notifications

Description

Time-to-live in seconds for notifications present in NOTIFICATION_LOG. Only used when Enable Stored Notifications in Database is enabled.

Related Name

hive.metastore.event.db.listener.timetolive

Default Value

2 day(s)

API Name

hive_metastore_event_db_listener_timetolive

Required

false

Hive Metastore Server Filter Hook

Description

Class name for the Hive Metastore Server Filter Hook. The class needs to implement the org.apache.hadoop.hive.metastore.MetastoreFilterHook interface.

Related Name

hive.metastore.filter.hook

Default Value

org.apache.hadoop.hive.ql.security.authorization.plugin.metastore.HiveMetaStoreAuthorizer

API Name

hive_metastore_filter_hook

Required

false

Enable Hive Metastore Server Filter

Description

When checked, the Hive Metastore Server will filter results based on the Filter Hook.

Related Name

hive.metastore.server.filter.enabled

Default Value

true

API Name

hive_metastore_server_filter_enabled

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Hive Metastore Server Port

Description

Port on which Hive Metastore Server will listen for connections.

Related Name

hive.metastore.port

Default Value

9083

API Name

hive_metastore_port

Required

false

Resource Management

Java Heap Size of Hive Metastore Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

8 GiB

API Name

hive_metastore_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the

value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user

with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Hive Metastore Max Message Size Validator

Description

Whether to suppress configuration warnings produced by the Hive Metastore Max Message Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hms_max_message_size_validator

Required

true

Suppress Parameter Validation: Hive Metastore Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Parameter Validation: Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_config_safety_valve

Required

true

Suppress Parameter Validation: Hive Metastore Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_env_safety_valve

Required

true

Suppress Parameter Validation: Hive Metastore Server Filter Hook

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Filter Hook parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_filter_hook

Required

true

Suppress Parameter Validation: Java Configuration Options for Hive Metastore Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Hive Metastore Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_java_opts

Required

true

Suppress Parameter Validation: Hive Metastore Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_port

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Parameter Validation: Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hms_core_site_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Hive Metastore Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_audit_health

Required

true

Suppress Health Test: Hive Metastore Canary

Description

Whether to suppress the results of the Hive Metastore Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_canary_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_pause_duration

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hivemetastore_unexpected_exits

Required

true

HiveServer2

Advanced

HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hive_hs2_config_safety_valve

Required

false

HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

hive_hs2_env_safety_valve

Required

false

Hive Metastore Connection Retries Count

Description

Number of retries while opening a connection to the Hive Metastore Server

Related Name

hive.metastore.connect.retries

Default Value

10

API Name

hive_metastore_connection_retries

Required

false

Enable Metrics Subsystem

Description

Controls whether the Hive metrics subsystem is enabled for the role.

Related Name

hive.server2.metrics.enabled

Default Value

true

API Name

hive_metrics_enabled

Required

false

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hive/metrics-hivemetastore/metrics.log. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.location

Default Value

API Name

hive_metrics_sample_file_location

Required

false

Metrics Sample File Logging Frequency

Description

The frequency at which the metrics are logged to the sample file. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.frequency

Default Value

30 second(s)

API Name

hive_metrics_sample_logging_frequency

Required

false

Hive Downloaded Resources Directory

Description

Local directory where Hive stores jars downloaded for remote file systems (HDFS). If not specified, Hive uses a default location.

Related Name

hive.downloaded.resources.dir

Default Value

API Name

hiveserver2_downloaded_resources_dir

Required

false

Enable Explain Logging

Description

When enabled, HiveServer2 logs EXPLAIN EXTENDED output for every query at INFO log4j level.

Related Name

hive.log.explain.output

Default Value

false

API Name

hiveserver2_enable_explain_output

Required

false

Hive Local Scratch Directory

Description

Local Directory where Hive stores jars and data when performing a MapJoin optimization. If not specified, Hive uses a default location.

Related Name

hive.exec.local.scratchdir

Default Value

API Name

hiveserver2_exec_local_scratchdir

Required

false

Hive HDFS Scratch Directory

Description

Directory in HDFS where Hive writes intermediate data between MapReduce jobs. If not specified, Hive uses a default location.

Related Name

hive.exec.scratchdir

Default Value

API Name

hiveserver2_exec_scratchdir

Required

false

Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

An XML string that will be inserted verbatim into the Fair Scheduler allocations file. This configuration only has effect in CDH 5.8 or later.

Related Name

Default Value

API Name

hiveserver2_fair_scheduler_safety_valve

Required

false

Idle Operation Timeout

Description

Operation will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero. For a positive value, checked for operations in terminal state only (FINISHED, CANCELED, CLOSED, ERROR). For a negative value, checked for all of the operations regardless of state.

Related Name

hive.server2.idle.operation.timeout

Default Value

6 hour(s)

API Name

hiveserver2_idle_operation_timeout

Required

false

Idle Session Timeout

Description

Session will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero or a negative value.

Related Name

hive.server2.idle.session.timeout

Default Value

1 day(s)

API Name

hiveserver2_idle_session_timeout

Required

false

Exclude Live Operations From Session Idle Time

Description

Session will be considered to be idle only if there is no activity, and there is no pending operation. This setting takes effect only if session idle timeout (hive.server2.idle.session.timeout) and checking (hive.server2.session.check.interval) are enabled.

Related Name

hive.server2.idle.session.check.operation

Default Value

true

API Name

hiveserver2_idle_session_timeout_check_operation

Required

false

Java Configuration Options for HiveServer2

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hiveserver2_java_opts

Required

false

Maximum Query String Length for Show Locks

Description

The maximum length allowed for the query string when the SHOW LOCKS EXTENDED command is executed. Important: The query string is truncated at the length set for this property. Setting this property to a large value puts pressure on ZooKeeper and might cause out-of-memory issues.

Related Name

hive.lock.query.string.max.length

Default Value

10000

API Name

hiveserver2_lock_query_string_max_length

Required

false

Max HiveServer2 Threads

Description

Maximum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.max.worker.threads

Default Value

500

API Name

hiveserver2_max_threads

Required

true

Min HiveServer2 Threads

Description

Minimum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.min.worker.threads

Default Value

5

API Name

hiveserver2_min_threads

Required

true

Session Check Interval

Description

The check interval for session/operation timeout, in milliseconds, which can be disabled by setting to zero or a negative value.

Related Name

hive.server2.session.check.interval

Default Value

15 minute(s)

API Name

hiveserver2_session_check_interval

Required

false

HiveServer2 WebUI Max Threads

Description

The max threads for the HiveServer2 WebUI.

Related Name

hive.server2.webui.max.threads

Default Value

50

API Name

hiveserver2_webui_max_threads

Required

false

HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

hs2_core_site_safety_valve

Required

false

HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HiveServer2 Log Directory

Description

Directory where HiveServer2 will place its log files.

Related Name

Default Value

/var/log/hive

API Name

hive_log_dir

Required

false

Enable Performance Logging

Description

When enabled, it captures time spent during each part of the query execution for the role.

Related Name

hive.server2.performance.logging.enabled

Default Value

true

API Name

hive_performance_logging_enabled

Required

false

Enable HiveServer2 Operations Logging

Description

When enabled, HiveServer2 will temporarily save logs associated with ongoing operations. This enables clients like beeline and Hue to request and display logs for a particular ongoing operation. Logs are removed upon completion of operation.

Related Name

hive.server2.logging.operation.enabled

Default Value

true

API Name

hive_server2_logging_operation_enabled

Required

false

HiveServer2 Operations Log Directory

Description

Top level directory where operation logs are temporarily stored if Enable HiveServer2 Operations Logging is true. Logs are stored in session and operation level subdirectories under this location and are removed on completion of operation.

Related Name

hive.server2.logging.operation.log.location

Default Value

/var/log/hive/operation_logs

API Name

hive_server2_logging_operation_log_location

Required

false

HiveServer2 Logging Threshold

Description

The minimum log level for HiveServer2 logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HiveServer2 Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HiveServer2 Max Log Size

Description

The maximum size, in megabytes, per log file for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hiveserver2_downloaded_resources_directory_free_space_absolute_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hiveserver2_downloaded_resources_directory_free_space_percentage_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hiveserver2_exec_local_scratch_directory_free_space_absolute_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hiveserver2_exec_local_scratch_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hiveserver2_fd_thresholds

Required

false

HiveServer2 Host Health Test

Description

When computing the overall HiveServer2 health, consider the host's health.

Related Name

Default Value

true

API Name

hiveserver2_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

hiveserver2_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

hiveserver2_pause_duration_window

Required

false

HiveServer2 Process Health Test

Description

Enables the health test that the HiveServer2's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hiveserver2_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11121

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'metrics<name=(jvm\.pause.*)><>(.*): (\d+)' name: $1_$2 value: $3

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: strict metric_names: #memory - jvm_buffer_pool_used_bytes - jvm_buffer_pool_capacity_bytes - jvm_buffer_pool_used_buffers - jvm_memory_bytes_used - jvm_memory_bytes_committed - jvm_memory_bytes_max - jvm_memory_bytes_init #gc - jvm_gc_collection_seconds #threads - jvm_threads_current - jvm_threads_daemon - jvm_threads_peak - jvm_threads_started_total - jvm_threads_deadlocked - jvm_threads_deadlocked_monitor - jvm_threads_state #classes - jvm_classes_currently_loaded #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes - jvm_pause_extrasleeptime_count

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Restrict Cross Joins (Cartesian Products)

Description

Whether to allow queries with cross joins. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.cartesian.product

Default Value

false

API Name

hive_restrict_cross_joins

Required

false

Restrict LOAD Queries Against Bucketed Tables

Description

Whether to allow LOAD queries against bucketed tables. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.bucketing

Default Value

true

API Name

hive_restrict_load_bucketed_table

Required

false

Restrict Queries with ORDER BY but no LIMIT clause

Description

Whether to allow queries with an ORDER BY clause, but no LIMIT clause. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.orderby.no.limit

Default Value

false

API Name

hive_restrict_orderby_with_no_limit

Required

false

Restrict Partitioned Table Scans with no Partitioned Column Filter

Description

Whether to allow queries that scan a partitioned table but don't filter on the partition column. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.no.partition.filter

Default Value

false

API Name

hive_restrict_partitioned_scans_no_filter

Required

false

Restrict Unsafe Data Type Comparisons

Description

Whether to allow queries that compare bigints to strings or doubles. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.type.safety

Default Value

true

API Name

hive_restrict_unsafe_comparison

Required

false

HiveServer2 Enable Impersonation

Description

HiveServer2 will impersonate the beeline client user when talking to other services such as MapReduce and HDFS.

Related Name

hive.server2.enable.doAs

Default Value

true

API Name

hiveserver2_enable_impersonation

Required

false

HiveServer2 Load Balancer

Description

Address of the load balancer used for HiveServer2 roles, specified in host:port format. If port is not specified, the port used by HiveServer2 is used. Note: Changing this property regenerates Kerberos keytabs for all HiveServer2 roles.

Related Name

Default Value

API Name

hiveserver2_load_balancer

Required

false

Performance

Hive Auto Convert Join Noconditional Size

Description

If Hive auto convert join is on, and the sum of the size for n-1 of the tables/partitions for a n-way join is smaller than the specified size, the join is directly converted to a MapJoin (there is no conditional task).

Related Name

hive.auto.convert.join.noconditionaltask.size

Default Value

50 MiB

API Name

hiveserver2_auto_convert_join_noconditionaltask_size

Required

false

Store Intermediate Data on Blobstore

Description

When writing data to a table on a blobstore (such as S3), whether or not the blobstore should be used to store intermediate data during Hive query execution. Setting this to true can degrade performance for queries that spawn multiple MR / Spark jobs, but is useful for queries whose intermediate data cannot fit in the allocated HDFS cluster.

Related Name

hive.blobstore.use.blobstore.as.scratchdir

Default Value

false

API Name

hiveserver2_blobstore_use_blobstore_as_scratchdir

Required

false

Enable Stats Optimization

Description

Enable optimization that checks if a query can be answered using statistics. If so, answers the query using only statistics stored in metastore.

Related Name

hive.compute.query.using.stats

Default Value

true

API Name

hiveserver2_compute_query_using_stats

Required

false

Enable Cost-Based Optimizer for Hive

Description

Enabled the Calcite-based Cost-Based Optimizer for HiveServer2.

Related Name

hive.cbo.enable

Default Value

true

API Name

hiveserver2_enable_cbo

Required

false

Enable MapJoin Optimization

Description

Enable optimization that converts common join into MapJoin based on input file size.

Related Name

hive.auto.convert.join

Default Value

true

API Name

hiveserver2_enable_mapjoin

Required

false

Fetch Task Query Conversion

Description

Some select queries can be converted to a single FETCH task instead of a MapReduce task, minimizing latency. A value of none disables all conversion, minimal converts simple queries such as SELECT * and filter on partition columns, and more converts SELECT queries including FILTERS.

Related Name

hive.fetch.task.conversion

Default Value

more

API Name

hiveserver2_fetch_task_conversion

Required

false

Fetch Task Query Conversion Threshold

Description

Above this size, queries are converted to fetch tasks.

Related Name

hive.fetch.task.conversion.threshold

Default Value

1 GiB

API Name

hiveserver2_fetch_task_conversion_threshold

Required

false

Input Listing Max Threads

Description

Maximum number of threads that Hive uses to list input files. Increasing this value can improve performance when there are a lot of partitions being read, or when running on blobstores.

Related Name

hive.exec.input.listing.max.threads

Default Value

15

API Name

hiveserver2_input_listing_max_threads

Required

false

Maximum ReduceSink Top-K Memory Usage

Description

The maximum percentage of heap to be used for hash in ReduceSink operator for Top-K selection. 0 means the optimization is disabled. Accepted values are between 0 and 1.

Related Name

hive.limit.pushdown.memory.usage

Default Value

0.04

API Name

hiveserver2_limit_pushdown_memory_usage

Required

false

Load Dynamic Partitions Thread Count

Description

Number of threads used to load dynamically generated partitions. Loading requires renaming the file its final location, and updating some metadata about the new partition. Increasing this can improve performance when there are a lot of partitions dynamically generated.

Related Name

hive.load.dynamic.partitions.thread

Default Value

15

API Name

hiveserver2_load_dynamic_partitions_thread_count

Required

false

Enable Map-Side Aggregation

Description

Enable map-side partial aggregation, which cause the mapper to generate fewer rows. This reduces the data to be sorted and distributed to reducers.

Related Name

hive.map.aggr

Default Value

true

API Name

hiveserver2_map_aggr

Required

false

Ratio of Memory Usage for Map-Side Aggregation

Description

Portion of total memory used in map-side partial aggregation. When exceeded, the partially aggregated results will be flushed from the map task to the reducers.

Related Name

hive.map.aggr.hash.percentmemory

Default Value

0.5

API Name

hiveserver2_map_aggr_hash_memory_ratio

Required

false

Enable Merging Small Files - Map-Only Job

Description

Merge small files at the end of a map-only job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapfiles

Default Value

true

API Name

hiveserver2_merge_mapfiles

Required

false

Enable Merging Small Files - Map-Reduce Job

Description

Merge small files at the end of a map-reduce job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapredfiles

Default Value

false

API Name

hiveserver2_merge_mapredfiles

Required

false

Desired File Size After Merging

Description

The desired file size after merging. This should be larger than hive.merge.smallfiles.avgsize.

Related Name

hive.merge.size.per.task

Default Value

256 MiB

API Name

hiveserver2_merge_size_per_task

Required

false

Small File Average Size Merge Threshold

Description

When the average output file size of a job is less than the value of this property, Hive will start an additional map-only job to merge the output files into bigger files. This is only done for map-only jobs if hive.merge.mapfiles is true, for map-reduce jobs if hive.merge.mapredfiles is true, and for Spark jobs if hive.merge.sparkfiles is true.

Related Name

hive.merge.smallfiles.avgsize

Default Value

16 MiB

API Name

hiveserver2_merge_smallfiles_avgsize

Required

false

MSCK Repair Batch Size

Description

Batch size for the msck repair command (recover partitions command). If the value is greater than zero, new partition information will be sent from HiveServer2 to the Metastore in batches, which can potentially improve memory usage in the Metastore and avoid client read timeout exceptions. If this value is 0, all partition information will sent in a single Thrift call.

Related Name

hive.msck.repair.batch.size

Default Value

3000

API Name

hiveserver2_msck_repair_batch_size

Required

false

Move Files Thread Count

Description

The number of threads used by HiveServer2 to move data from the staging directory to another location (typically to the final table location). A separate thread pool of workers of this size is used for each query, which means this configuration can be set on a per-query basis too.

Related Name

hive.mv.files.thread

Default Value

15

API Name

hiveserver2_mv_files_thread

Required

false

Hive Optimize Sorted Merge Bucket Join

Description

Whether to try sorted merge bucket (SMB) join.

Related Name

hive.optimize.bucketmapjoin.sortedmerge

Default Value

false

API Name

hiveserver2_optimize_bucketmapjoin_sortedmerge

Required

false

Enable Automatic Use of Indexes

Description

Whether to use the indexing optimization for all queries.

Related Name

hive.optimize.index.filter

Default Value

true

API Name

hiveserver2_optimize_index_filter

Required

false

Enable ReduceDeDuplication Optimization

Description

Remove extra map-reduce jobs if the data is already clustered by the same key, eliminating the need to repartition the dataset again.

Related Name

hive.optimize.reducededuplication

Default Value

true

API Name

hiveserver2_optimize_reducededuplication

Required

false

Mininum Reducers for ReduceDeDuplication Optimization

Description

When the number of ReduceSink operators after merging is less than this number, the ReduceDeDuplication optimization will be disabled.

Related Name

hive.optimize.reducededuplication.min.reducer

Default Value

4

API Name

hiveserver2_optimize_reducededuplication_min_reducer

Required

false

Enable Sorted Dynamic Partition Optimizer

Description

When dynamic partition is enabled, reducers keep only one record writer at all times, which lowers the memory pressure on reducers.

Related Name

hive.optimize.sort.dynamic.partition

Default Value

false

API Name

hiveserver2_optimize_sort_dynamic_partition

Required

false

Enable Parallel Compilation of Queries

Description

When activated, individual sessions can compile queries simultaneously. Within each session, queries compile one at a time.

Related Name

hive.driver.parallel.compilation

Default Value

true

API Name

hiveserver2_parallel_compilation_enabled

Required

false

Query Compilation Degree of Parallelism

Description

Determines the maximum number of queries that can compile in parallel on a HiveServer2 instance. Use negative values or zero to set unlimited parallelism. Use a positive value to set the number of queries that can compile simultaneously. This setting can be fine-tuned based on the current cluster load. Monitor cluster load using the 'waiting_compile_ops' metric and the 'Waiting Compile Operations' graph in the HiveServer2 graph library.

Related Name

hive.driver.parallel.compilation.global.limit

Default Value

5

API Name

hiveserver2_parallel_compilation_global_limit

Required

false

Hive SMB Join Cache Rows

Description

The number of rows with the same key value to be cached in memory per SMB-joined table.

Related Name

hive.smbjoin.cache.rows

Default Value

10000

API Name

hiveserver2_smbjoin_cache_rows

Required

false

Load Column Statistics

Description

Whether column stats for a table are fetched during explain.

Related Name

hive.stats.fetch.column.stats

Default Value

true

API Name

hiveserver2_stats_fetch_column_stats

Required

false

Sessions Per Queue

Description

The number of Tez sessions that should be launched on each of the queues specified by "hive.server2.tez.default.queues". Determines the parallelism on each queue.

Related Name

hive.server2.tez.sessions.per.default.queue

Default Value

4

API Name

hiveserver2_tez_sessions_per_default_queue

Required

false

Vectorized Adapter Usage Mode

Description

Vectorized Adaptor Usage Mode specifies the extent to which the vectorization engine tries to vectorize UDFs that do not have native vectorized versions available. Selecting the "none" option specifies that only queries using native vectorized UDFs are vectorized. Selecting the "chosen" option specifies that Hive choses to vectorize a subset of the UDFs based on performance benefits using the Vectorized Adaptor. Selecting the "all" option specifies that the Vectorized Adaptor be used for all UDFs even when native vectorized versions are not available.

Related Name

hive.vectorized.adaptor.usage.mode

Default Value

chosen

API Name

hiveserver2_vectorized_adaptor_usage_mode

Required

false

Enable Vectorization Optimization

Description

Enable optimization that vectorizes query execution by streamlining operations by processing a block of 1024 rows at a time.

Related Name

hive.vectorized.execution.enabled

Default Value

true

API Name

hiveserver2_vectorized_enabled

Required

false

Vectorized GroupBy Check Interval

Description

In vectorized group-by, the number of row entries added to the hash table before re-checking average variable size for memory usage estimation.

Related Name

hive.vectorized.groupby.checkinterval

Default Value

4096

API Name

hiveserver2_vectorized_groupby_checkinterval

Required

false

Vectorized GroupBy Flush Ratio

Description

Ratio between 0.0 and 1.0 of entries in the vectorized group-by aggregation hash that is flushed when the memory threshold is exceeded.

Related Name

hive.vectorized.groupby.flush.percent

Default Value

0.1

API Name

hiveserver2_vectorized_groupby_flush_ratio

Required

false

Enable Vectorized Input Format

Description

If enabled, Hive uses the native vectorized input format for vectorized query execution when it is available.

Related Name

hive.vectorized.use.vectorized.input.format

Default Value

true

API Name

hiveserver2_vectorized_input_format_enabled

Required

false

Exclude Vectorized Input Formats

Description

Specifies a list of file input format classnames to exclude from vectorized query execution using the vectorized input format. Note that vectorized execution can still occur for an excluded input format based on whether row SerDes or vector SerDes are enabled.

Related Name

hive.vectorized.input.format.excludes

Default Value

API Name

hiveserver2_vectorized_input_format_excludes

Required

false

Enable Reduce-Side Vectorization

Description

Whether to vectorize the reduce side of query execution.

Related Name

hive.vectorized.execution.reduce.enabled

Default Value

true

API Name

hiveserver2_vectorized_reduce_enabled

Required

false

Enable Overflow-checked Vector Expressions

Description

To enhance performance, vectorized expressions operate using wide data types like long and double. When wide data types are used, numeric overflows can occur during expression evaluation in a different manner for vectorized expressions than they do for non-vectorized expressions. Consequently, different query results can be returned for vectorized expressions compared to results returned for non-vectorized expressions. When this configuration is enabled, Hive uses vectorized expressions that handle numeric overflows in the same way as non-vectorized expressions are handled.

Related Name

hive.vectorized.use.checked.expressions

Default Value

true

API Name

hiveserver2_vectorized_use_checked_expressions

Required

false

Vectorize Using Vector SerDes

Description

If enabled, Hive uses built-in vector SerDes to process text and sequencefile tables for vectorized query execution.

Related Name

hive.vectorized.use.vector.serde.deserialize

Default Value

false

API Name

hiveserver2_vectorized_use_vector_serde_deserialize

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Bind HiveServer2 to Wildcard Address

Description

If enabled, the HiveServer2 binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

hive.server2.webui.host

Default Value

true

API Name

hiveserver2_webui_bind_wildcard

Required

false

HiveServer2 WebUI Port

Description

The port the HiveServer2 WebUI will listen on. This can be set to 0 to disable the WebUI.

Related Name

hive.server2.webui.port

Default Value

10002

API Name

hiveserver2_webui_port

Required

false

HiveServer2 Port

Description

Port on which HiveServer2 will listen for connections.

Related Name

hive.server2.thrift.port

Default Value

10000

API Name

hs2_thrift_address_port

Required

false

Resource Management

Java Heap Size of HiveServer2 in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

hiveserver2_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

HiveServer2 WebUI SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from WebUI SSL.

Related Name

hive.server2.webui.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_webui_exclude_ciphersuites

Required

false

Enable TLS/SSL for HiveServer2 WebUI

Description

Encrypt communication between clients and HiveServer2 WebUI using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.webui.use.ssl

Default Value

false

API Name

ssl_enabled

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 WebUI is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.webui.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 WebUI keystore file.

Related Name

hive.server2.webui.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_config_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Parameter Validation: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Operations Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Parameter Validation: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Downloaded Resources Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Parameter Validation: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Local Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Parameter Validation: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive HDFS Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Parameter Validation: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HiveServer2 parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Parameter Validation: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Parameter Validation: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Vectorized Input Formats parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Parameter Validation: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_audit_health

Required

true

Suppress Health Test: Hive Downloaded Resources Directory Free Space

Description

Whether to suppress the results of the Hive Downloaded Resources Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_downloaded_resources_directory_free_space

Required

true

Suppress Health Test: Hive Local Scratch Directory Free Space

Description

Whether to suppress the results of the Hive Local Scratch Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_exec_local_scratch_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_pause_duration

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hiveserver2_unexpected_exits

Required

true

Service-Wide

Advanced

Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

For advanced use only, a string to be inserted into atlas-application.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

application_properties_safety_valve

Required

false

Hive Auxiliary JARs Directory

Description

Directory containing auxiliary JARs used by Hive. This should be a directory location and not a classpath containing one or more JARs. This directory must be created and managed manually on hosts that run the Hive Metastore Server, HiveServer2, or the Hive CLI. The directory location is set in the environment as HIVE_AUX_JARS_PATH and will generally override the hive.aux.jars.path property set in XML files, even if hive.aux.jars.path is set in an advanced configuration snippet.

Related Name

Default Value

API Name

hive_aux_jars_path_dir

Required

false

Bypass Hive Metastore Server

Description

Instead of talking to Hive Metastore Server for Metastore information, Hive clients will talk directly to the Metastore database.

Related Name

Default Value

false

API Name

hive_bypass_metastore_server

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_core_site_safety_valve

Required

false

Hive Copy Large File Size

Description

Smaller than this size, Hive uses a single-threaded copy; larger than this size, Hive uses DistCp.

Related Name

hive.exec.copyfile.maxsize

Default Value

32 MiB

API Name

hive_exec_copyfile_maxsize

Required

false

Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the environment of Hive replication jobs.

Related Name

Default Value

API Name

hive_replication_env_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml

Description

For advanced use only, a string to be inserted into sentry-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_server2_sentry_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_service_config_safety_valve

Required

false

Hive Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_service_env_safety_valve

Required

false

Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to all Hive Replication jobs.

Related Name

Default Value

API Name

hive_service_replication_config_safety_valve

Required

false

Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.lineage.client.properties.

Related Name

Default Value

API Name

navigator_lineage_client_config_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_username

Required

true

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

For advanced use only, a string to be inserted into ranger-hive-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-hive-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

For advanced use only, a string to be inserted into ranger-hive-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for Hive events:

- userName: the user performing the action.
- ipAddress: the IP from where the request originated.
- operation: the Hive operation being performed.

- databaseName: the databaseName for the operation.
- tableName: the tableName for the operation.

The default Hive audit event filter discards HDFS directory events generated by Hive jobs that reference the /tmp directory.

Related Name

navigator.event.filter

Default Value

comment: [The default Hive audit event filter discards HDFS directory events , generated by Hive jobs that reference the /tmp directory.], defaultAction: accept, rules: [action: discard, fields: [name: operation, match: QUERY , name: objectType, match: DFS_DIR , name: resourcePath, match: /tmp/hive-(?:.+)?/hive_(?:.+)?/-mr-.*]]

API Name

navigator_audit_event_filter

Required

false

Audit Queue Policy

Description

Action to take when the audit event queue is full. Drop the event or shutdown the affected process.

Related Name

navigator.batch.queue_policy

Default Value

DROP

API Name

navigator_audit_queue_policy

Required

false

Audit Event Tracker

Description

Configures the rules for event tracking and coalescing. This feature is used to define equivalency between different audit events. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the "tracked" events according to the rules defined here. Event trackers are defined in a JSON object like the following: { "timeToLive" : [integer], "fields" : [{ "type" : [string], "name" : [string] }] } Where:

- timeToLive: maximum amount of time an event will be tracked, in milliseconds. Must be provided. This defines how long, since it's first seen, an event will be tracked. A value of 0 disables tracking.
- fields: list of fields to compare when matching events against tracked events.

Each field has an evaluator type associated with it. The evaluator defines how the field data is to be compared. The following evaluators are available:

- value: uses the field value for comparison.
- userName: treats the field value as a userNname, and ignores any host-specific data. This is useful for environment using Kerberos, so that only the principal name and realm are compared.

The following is the list of fields that can be used to compare Hive events:

- operation: the Hive operation being performed.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- databaseName: the database affected by the operation.
- tableName: the table or view affected by the operation.
- objectType: the type of object affected by the operation.
- resourcePath: the path of the resource affected by the operation.

Related Name

navigator_event_tracker

Default Value

API Name

navigator_event_tracker

Required

false

Enable Lineage Collection

Description

Enable collection of lineage from the service's roles.

Related Name

Default Value

true

API Name

navigator_lineage_enabled

Required

false

Database

Auto Create and Upgrade Hive Metastore Database Schema

Description

Automatically create or upgrade tables in the Hive Metastore database when needed. Consider setting this to false and managing the schema manually.

Related Name

datanucleus.schema.autoCreateAll

Default Value

false

API Name

hive_metastore_database_auto_create_schema

Required

false

Hive Metastore Database DataNucleus Metadata Validation

Description

Perform DataNucleus validation of metadata during startup. Note: when enabled, Hive will log DataNucleus warnings even though Hive will function normally.

Related Name

datanucleus.metadata.xml.validate

Default Value

false

API Name

hive_metastore_database_datanucleus_metadata_validation

Required

false

Enable Direct SQL

Description

Whether Hive Metastore should try to use direct SQL queries instead of DataNucleus for certain read paths. This can improve metastore performance by orders of magnitude when fetching many partitions. In case of failure, execution will fall back to DataNucleus.

Related Name

hive.metastore.try.direct.sql

Default Value

true

API Name

hive_metastore_database_datanucleus_try_direct_sql

Required

false

Hive Metastore Database Host

Description

Host name of Hive Metastore database

Related Name

Default Value

localhost

API Name

hive_metastore_database_host

Required

false

Hive Metastore Database Name

Description

Name of Hive Metastore database

Related Name

Default Value

metastore

API Name

hive_metastore_database_name

Required

false

Hive Metastore Database Password

Description

Password for Hive Metastore database

Related Name

javax.jdo.option.ConnectionPassword

Default Value

API Name

hive_metastore_database_password

Required

false

Hive Metastore Database Port

Description

Port number of Hive Metastore database

Related Name

Default Value

3306

API Name

hive_metastore_database_port

Required

false

Hive Metastore Database Type

Description

Type of Hive Metastore database. Note that Derby is not recommended and Apache Impala does not support Derby.

Related Name

Default Value

mysql

API Name

hive_metastore_database_type

Required

false

Hive Metastore Database User

Description

User for Hive Metastore database

Related Name

javax.jdo.option.ConnectionUserName

Default Value

hive

API Name

hive_metastore_database_user

Required

false

Hive Metastore Derby Path

Description

Directory name where Hive Metastore's database is stored (only for Derby)

Related Name

Default Value

/var/lib/hive/cloudera_manager/derby/metastore_db

API Name

hive_metastore_derby_path

Required

false

Strict Hive Metastore Schema Validation

Description

Prevent Metastore operations in the event of schema version incompatibility. Consider setting this to true to reduce probability of schema corruption during Metastore operations. Note that setting this property to true will also set datanucleus.autoCreateSchema property to false and datanucleus.fixedDatastore property to true. Any values set in Cloudera Manager for these properties will be overridden.

Related Name

hive.metastore.schema.verification

Default Value

true

API Name

hive_metastore_schema_verification

Required

false

Hive Metastore Database JDBC URL Override

Description

Custom JDBC URL to use when connecting to the Hive Metastore Database. This connection string will override all other values used to construct the JDBC URL, including Hive Metastore Database Host, Hive Metastore Database Name, and Hive Metastore Database Port.

Related Name

javax.jdo.option.ConnectionURL

Default Value

API Name

jdbc_url_override

Required

false

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/hive/audit

API Name

audit_event_log_dir

Required

false

Hive Lineage Log Directory

Description

The directory in which Hive lineage log files are written.

Related Name

lineage_event_log_dir

Default Value

/var/log/hive/lineage

API Name

lineage_event_log_dir

Required

true

Hive Maximum Lineage Log File Size

Description

The maximum size, in megabytes, per log file for Hive lineage logs. Typically used by log4j or logback.

Related Name

max_lineage_log_file_size

Default Value

100 MiB

API Name

max_lineage_log_file_size

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Number of Audit Logs to Retain

Description

Maximum number of rolled-over audit logs to retain. The logs are not deleted if they contain audit events that have not yet been propagated to the Audit Server.

Related Name

navigator.client.max_num_audit_log

Default Value

10

API Name

navigator_client_max_num_audit_log

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Failed Compaction Thresholds

Description

The health test thresholds for the number of failed compactions.

Related Name

Default Value

Warning: 1.0 %, Critical: Never

API Name

hive_compaction_failed_thresholds

Required

false

Hive Compaction Health Test

Description

Enables the health test that checks whether compaction processes are properly configured and operational.

Related Name

Default Value

false

API Name

hive_compaction_health_check_enabled

Required

false

Oldest Initiated Compaction Thresholds

Description

The health test thresholds for the oldest initiated compaction.

Related Name

Default Value

Warning: 1 hour(s), Critical: 12 hour(s)

API Name

hive_compaction_oldest_initiated_thresholds

Required

false

Healthy Hive Metastore Server Monitoring Thresholds

Description

The health test thresholds of the overall Hive Metastore Server health. The check returns "Concerning" health if the percentage of "Healthy" Hive Metastore Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Hive Metastore Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hive_hivemetastores_healthy_thresholds

Required

false

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hive_hiveserver2s_healthy_thresholds

Required

false

Healthy WebHCat Server Monitoring Thresholds

Description

The health test thresholds of the overall WebHCat Server health. The check returns "Concerning" health if the percentage of "Healthy" WebHCat Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" WebHCat Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hive_webhcats_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "I F (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", " streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on

how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>hive.metastore.client.socket.timeout</name> <value>60</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Atlas Service

Description

Name of the Atlas service that this Hive service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Generate HADOOP_CREDSTORE_PASSWORD

Description

Flag to enable or disable the generation of HADOOP_CREDSTORE_PASSWORD.

Related Name

generate_jceks_password

Default Value

true

API Name

generate_jceks_password

Required

false

HBase Service

Description

Name of the HBase service that this Hive service instance depends on.

Related Name

Default Value

API Name

hbase_service

Required

false

HDFS Service

Description

Name of the HDFS service that this Hive service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Enable Asynchronous Logging

Description

Asynchronous Log4j2 logging can give a significant performance improvement as logging will be handled in a separate thread that uses an LMAX disruptor queue for buffering log messages. Refer to https://logging.apache.org/log4j/2.x/manual/async.html for benefits and drawbacks. For debugging issues we recommend setting this to false.

Related Name

hive.async.log.enabled

Default Value

false

API Name

hive_async_log_enabled

Required

false

Hive Bytes Per Reducer

Description

Size per reducer. If the input size is 10GiB and this is set to 1GiB, Hive will use 10 reducers.

Related Name

hive.exec.reducers.bytes.per.reducer

Default Value

64 MiB

API Name

hive_bytes_per_reducer

Required

false

Enable Metastore Notifications for DML Operations

Description

When set to true, DML queries from Hive (and SparkSQL for limited use-cases) which insert data into tables will fire listener notifications in the metastore.

Related Name

hive.metastore.dml.events

Default Value

true

API Name

hive_fire_events_for_dml

Required

false

Hive Max Reducers

Description

Max number of reducers to use. If the configuration parameter Hive Reduce Tasks is negative, Hive will limit the number of reducers to the value of this parameter.

Related Name

hive.exec.reducers.max

Default Value

1009

API Name

hive_max_reducers

Required

false

Hive Reduce Tasks

Description

Default number of reduce tasks per job. Usually set to a prime number close to the number of available hosts. Ignored when mapred.job.tracker is "local". Hadoop sets this to 1 by default, while

Hive uses -1 as the default. When set to -1, Hive will automatically determine an appropriate number of reducers for each job.

Related Name

mapred.reduce.tasks

Default Value

-1

API Name

hive_reduce_tasks

Required

false

Support Dynamic Service Discovery

Description

Whether HiveServer2 supports dynamic service discovery for its clients. To support this, each instance of HiveServer2 currently uses ZooKeeper to register itself, when it is brought up. JDBC/ODBC clients should use the ZooKeeper ensemble: hive.zookeeper.quorum in their connection string.

Related Name

hive.server2.support.dynamic.service.discovery

Default Value

true

API Name

hive_server2_support_dynamic_service_discovery

Required

false

Set User and Group Information

Description

In unsecure mode, setting this property to true will cause the Metastore Server to execute DFS operations using the client's reported user and group permissions. Cloudera Manager will set this for all clients and servers.

Related Name

hive.metastore.execute.setugi

Default Value

true

API Name

hive_set_ugi

Required

true

Hive Warehouse Directory

Description

Hive warehouse directory is the location in HDFS where Hive's tables are stored. Note that Hive's default value for its warehouse directory is '/user/hive/warehouse'.

Related Name

hive.metastore.warehouse.dir

Default Value

/warehouse/tablespace/managed/hive

API Name

hive_warehouse_directory

Required

false

Hive External Warehouse Directory

Description

Hive external warehouse directory is the location in HDFS where Hive's tables are stored. Note that Hive's default value for its warehouse directory is '/user/hive/warehouse'.

Related Name

hive.metastore.warehouse.external.dir

Default Value

/warehouse/tablespace/external/hive

API Name

hive_warehouse_external_directory

Required

false

LDAP password

Description

LDAP password for Hive 3 replication

Related Name

Default Value

API Name

hiveserver2_ldap_replication_password

Required

false

LDAP username

Description

LDAP username for Hive 3 replication

Related Name

Default Value

API Name

hiveserver2_ldap_replication_user

Required

false

MapReduce Service

Description

MapReduce jobs are run against this service.

Related Name

Default Value

API Name

mapreduce_yarn_service

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hive.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin URL Auth Filesystem Schemes

Description

Set Ranger URL Auth Filesystem Schemes.

Related Name

ranger.plugin.hive.urlauth.filesystem.schemes

Default Value

hdfs:, file:, wasb:, adl:

API Name

ranger_plugin_urlauth_filesystem_schemes

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hive.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Hive service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Hive service instance depends on.

Related Name

Default Value

API Name

zookeeper_service

Required

false

Performance

Metastore Bulk Partitions Thread Count

Description

The number of threads the metastore uses when bulk adding partitions to the metastore.. Each thread performs some metadata operations for each partition added, such as collecting statistics for the partition or checking if the partition directory exists. This config is also used to control the size of the threadpool used when scanning the filesystem to look for directories that could correspond to partitions, each thread performs a list status on each possible partition directory.

Related Name

hive.metastore.fshandler.threads

Default Value

15

API Name

hive_metastore_fshandler_threads

Required

false

Policy File Based Sentry

Sentry User to Group Mapping Class

Description

The class to use in Sentry authorization for user to group mapping. Sentry authorization may be configured to use either Hadoop user to group mapping or local groups defined in the policy file. Hadoop user to group mapping may be configured in the Cloudera Manager HDFS service configuration page under the Security section.

Related Name

hive.sentry.provider

Default Value

org.apache.sentry.provider.file.HadoopGroupResourceAuthorizationProvider

API Name

hive_sentry_provider

Required

false

Sentry Global Policy File

Description

HDFS path to the global policy file for Sentry authorization. This should be a relative path (and not a full HDFS URL). The global policy file must be in Sentry policy file format.

Related Name

hive.sentry.provider.resource

Default Value

/user/hive/sentry/sentry-provider.ini

API Name

hive_sentry_provider_resource

Required

false

Allow URIs in Database Policy File

Description

Allows URIs when defining privileges in per-database policy files. Warning: Typically, this configuration should be disabled. Enabling it would allow database policy file owner (which is generally not Hive admin user) to grant load privileges to any directory with read access to Hive admin user, including databases controlled by other database policy files.

Related Name

sentry.allow.uri.db.policyfile

Default Value

false

API Name

sentry_allow_uri_db_policyfile

Required

false

Proxy

Hive Metastore Access Control and Proxy User Groups Override

Description

This configuration overrides the value set for Hive Proxy User Groups configuration in HDFS service for use by Hive Metastore Server. Specify a comma-delimited list of groups that you want to allow access to Hive Metastore metadata and allow the Hive user to impersonate. A value of '*' allows all groups. The default value of empty inherits the value set for Hive Proxy User Groups configuration in the HDFS service.

Related Name

hadoop.proxyuser.hive.groups

Default Value

API Name

hive_proxy_user_groups_list

Required

false

Hive Metastore Access Control and Ranger RMS Proxy User Hosts

Description

Comma-delimited list of hosts that you want to allow access to Hive Metastore metadata and allow the Ranger RMS user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.rangerrms.hosts

Default Value

*

API Name

rangerrms_proxy_user_hosts_list

Required

false

Replication

Replica functions root directory

Description

Root directory on the replica warehouse where the repl sub-system will store jars from the primary warehouse

Related Name

hive.repl.replica.functions.root.dir

Default Value

API Name

hive_repl_replica_functions_root_dir

Required

false

Security

Atlas Kafka Messages Spool Directory

Description

Spool directory for Atlas Kafka Messages.

Related Name

atlas.hook.spool.dir

Default Value

/var/log/hive/atlas-spool

API Name

atlas_message_spool_path

Required

false

Enable LDAP Authentication for Hive Metastore

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

Default Value

false

API Name

hive_metastore_enable_ldap_auth

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like "uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

hive.metastore.authentication.ldap.baseDN

Default Value

API Name

hive_metastore_ldap_basedn

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

hive.metastore.authentication.ldap.Domain

Default Value

API Name

hive_metastore_ldap_domain

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used,

and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

hive.metastore.authentication.ldap.url

Default Value

API Name

hive_metastore_ldap_uri

Required

false

Enable LDAP Authentication for HiveServer2

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

Default Value

false

API Name

hiveserver2_enable_ldap_auth

Required

false

Enable TLS/SSL for HiveServer2

Description

Encrypt communication between clients and HiveServer2 using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.use.SSL

Default Value

false

API Name

hiveserver2_enable_ssl

Required

false

HiveServer2 SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from Hiveserver2 SSL.

Related Name

hive.server2.http.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_exclude_ciphersuites

Required

false

HiveServer2 SSL Include Cipher Suites

Description

The cipher suites should be included in Hiverserver2 SSL.

Related Name

hive.server2.binary.include.ciphersuites

Default Value

modern2018

API Name

hiveserver2_include_ciphersuites

Required

false

HiveServer2 TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 keystore file.

Related Name

hive.server2.keystore.password

Default Value

API Name

hiveserver2_keystore_password

Required

false

HiveServer2 TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.keystore.path

Default Value

API Name

hiveserver2_keystore_path

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like

"uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

hive.server2.authentication.ldap.baseDN

Default Value

API Name

hiveserver2_ldap_basedn

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

hive.server2.authentication.ldap.Domain

Default Value

API Name

hiveserver2_ldap_domain

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

hive.server2.authentication.ldap.url

Default Value

API Name

hiveserver2_ldap_uri

Required

false

HiveServer2 TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HiveServer2 might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

hiveserver2_truststore_file

Required

false

HiveServer2 TLS/SSL Trust Store Password

Description

The password for the HiveServer2 TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

hiveserver2_truststore_password

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hive

API Name

kerberos_princ_name

Required

true

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hive

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hive/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hive/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hive.policy.cache.dir

Default Value

/var/lib/ranger/hive/policy-cache

API Name

ranger_policy_cache_dir

Required

false

Bypass Sentry Authorization Users

Description

List of users that are allowed to bypass Sentry Authorization in the Hive metastore. These are usually service users that already ensure that all activity has been authorized, such as hive and impala. Only applies when Hive is using Sentry Service.

Related Name

sentry.metastore.service.users

Default Value

hive impala hue hdfs

API Name

sentry_metastore_service_users

Required

false

Hive Metastore TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Hive Metastore might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

hive.metastore.dbaccess.ssl.truststore.path

Default Value

API Name

ssl_client_truststore_location

Required

false

Hive Metastore TLS/SSL Trust Store Password

Description

The password for the Hive Metastore TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

hive.metastore.dbaccess.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL to the Hive Metastore Database

Description

Encrypt communication between Hive Metastore and the database using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)). If this is enabled, then the optionally provided Hive Metastore TLS/SSL Client Trust Store properties will be used.

Related Name

hive.metastore.dbaccess.ssl.use.SSL

Default Value

false

API Name

ssl_enabled_database

Required

false

Sentry HDFS Sync Cache

Abort on Initialization Failure

Description

If set to true, the Hive metastore will treat a problem with cache initialization as a fatal error.

Related Name

sentry.hdfs.sync.metastore.cache.fail.on.partial.update

Default Value

true

API Name

sentry_hdfs_sync_metastore_cache_fail_on_partial_update

Required

false

Number of Threads on Initialization

Description

The number of threads used during Hive Metastore Sentry HDFS Sync Cache Initialization.

Related Name

sentry.hdfs.sync.metastore.cache.init.threads

Default Value

10

API Name

sentry_hdfs_sync_metastore_cache_init_threads

Required

false

Number of Partitions per RPC on Initialization

Description

The number of partitions per RPC retrieved during Hive Metastore Sentry HDFS Sync Cache Initialization.

Related Name

sentry.hdfs.sync.metastore.cache.max-partitions-per-rpc

Default Value

100

API Name

sentry_hdfs_sync_metastore_cache_partitions_per_rpc

Required

false

Max Number of Retries on Initialization

Description

The maximum number of retries allowed during Hive Metastore Sentry HDFS Sync cache initialization.

Related Name

sentry.hdfs.sync.metastore.cache.retry.max.num

Default Value

1

API Name

sentry_hdfs_sync_metastore_cache_retry_max_num

Required

false

Retry Wait Time on Initialization

Description

Wait duration in milliseconds for each retry during Hive Metastore Sentry HDFS Sync Cache Initialization.

Related Name

sentry.hdfs.sync.metastore.cache.retry.wait.duration.millis

Default Value

1 second(s)

API Name

sentry_hdfs_sync_metastore_cache_retry_wait_duration_millis

Required

false

Number of Tables per RPC on Initialization

Description

The number of tables per RPC retrieved during Hive Metastore Sentry HDFS Sync Cache Initialization.

Related Name

sentry.hdfs.sync.metastore.cache.max-tables-per-rpc

Default Value

100

API Name

sentry_hdfs_sync_metastore_cache_tables_per_rpc

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: WebHCat Server Log Directory

Description

Whether to suppress configuration warnings produced by the WebHCat Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hcatalog_log_dir

Required

true

Suppress Configuration Validator: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Configuration Validator: Hive Metastore Max Message Size Validator

Description

Whether to suppress configuration warnings produced by the Hive Metastore Max Message Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hms_max_message_size_validator

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_config_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Configuration Validator: Hive Metastore Server Log Directory

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Configuration Validator: Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_config_safety_valve

Required

true

Suppress Configuration Validator: Hive Metastore Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_env_safety_valve

Required

true

Suppress Configuration Validator: Hive Metastore Server Filter Hook

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Filter Hook configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_filter_hook

Required

true

Suppress Configuration Validator: Java Configuration Options for Hive Metastore Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Hive Metastore Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_java_opts

Required

true

Suppress Configuration Validator: Hive Metastore Server Port

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metastore_port

Required

true

Suppress Configuration Validator: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the Metrics Sample File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Configuration Validator: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the HiveServer2 Operations Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Configuration Validator: WebHCat Server Port

Description

Whether to suppress configuration warnings produced by the WebHCat Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_address_port

Required

true

Suppress Configuration Validator: WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml

Description

Whether to suppress configuration warnings produced by the WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_config_safety_valve

Required

true

Suppress Configuration Validator: WebHCat Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the WebHCat Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_env_safety_valve

Required

true

Suppress Configuration Validator: WebHCat Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the WebHCat Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_hive_config_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for WebHCat Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for WebHCat Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_java_opts

Required

true

Suppress Configuration Validator: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the Hive Downloaded Resources Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Configuration Validator: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive Local Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Configuration Validator: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive HDFS Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Configuration Validator: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HiveServer2 configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Configuration Validator: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the HiveServer2 Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Configuration Validator: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the Exclude Vectorized Input Formats configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Configuration Validator: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Configuration Validator: Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hms_core_site_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: WebHCat Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the WebHCat Server Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webhcat_core_site_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_application_properties_safety_valve

Required

true

Suppress Parameter Validation: Atlas Kafka Messages Spool Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Kafka Messages Spool Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_message_spool_path

Required

true

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Hive Auxiliary JARs Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Auxiliary JARs Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_aux_jars_path_dir

Required

true

Suppress Configuration Validator: Hive Bypass Metastore Validator

Description

Whether to suppress configuration warnings produced by the Hive Bypass Metastore Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_bypass_metastore_validator

Required

true

Suppress Configuration Validator: Client TLS/SSL In Use With LDAP Authentication Validator

Description

Whether to suppress configuration warnings produced by the Client TLS/SSL In Use With LDAP Authentication Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_client_ssl_recommended_with_ldap_auth_validator

Required

true

Suppress Configuration Validator: Hive Concurrency Configuration Validator

Description

Whether to suppress configuration warnings produced by the Hive Concurrency Configuration Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_concurrency_validator

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_core_site_safety_valve

Required

true

Suppress Configuration Validator: Hive Derby Validator

Description

Whether to suppress configuration warnings produced by the Hive Derby Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_derby_validator

Required

true

Suppress Parameter Validation: Hive Metastore Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database Host parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_host

Required

true

Suppress Parameter Validation: Hive Metastore Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_name

Required

true

Suppress Parameter Validation: Hive Metastore Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_password

Required

true

Suppress Parameter Validation: Hive Metastore Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_port

Required

true

Suppress Configuration Validator: Database TLS with JDBC URL Override Validator

Description

Whether to suppress configuration warnings produced by the Database TLS with JDBC URL Override Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_tls_overridden_by_jdbc_url_validator

Required

true

Suppress Parameter Validation: Hive Metastore Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_database_user

Required

true

Suppress Parameter Validation: Hive Metastore Derby Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Derby Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_derby_path

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_ldap_basedn

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_ldap_domain

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_ldap_uri

Required

true

Suppress Configuration Validator: Legacy HS2 Validator

Description

Whether to suppress configuration warnings produced by the Legacy HS2 Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_no_legacy_hs2_validator

Required

true

Suppress Configuration Validator: Hive Proxy Groups Validator

Description

Whether to suppress configuration warnings produced by the Hive Proxy Groups Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_groups_validator

Required

true

Suppress Parameter Validation: Hive Metastore Access Control and Proxy User Groups Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Access Control and Proxy User Groups Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_user_groups_list

Required

true

Suppress Configuration Validator: Ranger Plugin Url Auth Validator for filesystem schemes

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Url Auth Validator for filesystem schemes configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_url_auth_validator

Required

true

Suppress Configuration Validator: Hive Ranger Validator

Description

Whether to suppress configuration warnings produced by the Hive Ranger Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_validator

Required

true

Suppress Parameter Validation: Replica functions root directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replica functions root directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_repl_replica_functions_root_dir

Required

true

Suppress Parameter Validation: Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_replication_env_safety_valve

Required

true

Suppress Parameter Validation: Sentry Global Policy File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Sentry Global Policy File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_sentry_provider_resource

Required

true

Suppress Configuration Validator: Hive Sentry Validator

Description

Whether to suppress configuration warnings produced by the Hive Sentry Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_sentry_validator

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_server2_sentry_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_config_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_env_safety_valve

Required

true

Suppress Parameter Validation: Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_replication_config_safety_valve

Required

true

Suppress Parameter Validation: Hive Warehouse Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Warehouse Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_warehouse_directory

Required

true

Suppress Parameter Validation: Hive External Warehouse Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive External Warehouse Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_warehouse_external_directory

Required

true

Suppress Configuration Validator: Hive Metastore Server Count Validator

Description

Whether to suppress configuration warnings produced by the Hive Metastore Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hivemetastore_count_validator

Required

true

Suppress Configuration Validator: HiveServer2 Count Validator

Description

Whether to suppress configuration warnings produced by the HiveServer2 Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_count_validator

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_password

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_path

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_basedn

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_domain

Required

true

Suppress Parameter Validation: LDAP password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_replication_password

Required

true

Suppress Parameter Validation: LDAP username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP username parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_replication_user

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_uri

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_file

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_password

Required

true

Suppress Parameter Validation: Hive Metastore Database JDBC URL Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Database JDBC URL Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_jdbc_url_override

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Hive Lineage Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Lineage Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_lineage_event_log_dir

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Audit Event Tracker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Tracker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_event_tracker

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_lineage_client_config_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Plugin URL Auth Filesystem Schemes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin URL Auth Filesystem Schemes parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_urlauth_filesystem_schemes

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Parameter Validation: Hive Metastore Access Control and Ranger RMS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Access Control and Ranger RMS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_rangerrms_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Bypass Sentry Authorization Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Bypass Sentry Authorization Users parameter.

Related Name

Default Value

false

API Name

service_config_suppression_sentry_metastore_service_users

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Hive Metastore TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Hive Metastore TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: WebHCat Server Count Validator

Description

Whether to suppress configuration warnings produced by the WebHCat Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_webhcat_count_validator

Required

true

Suppress Health Test: Compaction System Health Check

Description

Whether to suppress the results of the Compaction System Health Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_compaction_health

Required

true

Suppress Health Test: Hive Metastore Server Health

Description

Whether to suppress the results of the Hive Metastore Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_hivemetastores_healthy

Required

true

Suppress Health Test: HiveServer2 Health

Description

Whether to suppress the results of the HiveServer2 Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_hiveserver2s_healthy

Required

true

Suppress Health Test: WebHCat Server Health

Description

Whether to suppress the results of the WebHCat Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_webhcats_healthy

Required

true

WebHCat Server

Advanced

WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml

Description

For advanced use only. A string to be inserted into webhcat-site.xml for this role only.

Related Name

Default Value

API Name

hive_webhcat_config_safety_valve

Required

false

WebHCat Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

hive_webhcat_env_safety_valve

Required

false

WebHCat Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hive_webhcat_hive_config_safety_valve

Required

false

Java Configuration Options for WebHCat Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hive_webhcat_java_opts

Required

false

WebHCat Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among

multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

WebHCat Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

webhcat_core_site_safety_valve

Required

false

Logs

WebHCat Server Log Directory

Description

Directory where WebHCat Server will place its log files.

Related Name

Default Value

/var/log/hcatalog

API Name

hcatalog_log_dir

Required

false

WebHCat Server Logging Threshold

Description

The minimum log level for WebHCat Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

WebHCat Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for WebHCat Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

WebHCat Server Max Log Size

Description

The maximum size, in megabytes, per log file for WebHCat Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: '^nothing-should-match-this$'

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: strict metric_names: #memory - jvm_buffer_pool_used_bytes - jvm_buffer_pool_capacity_bytes - jvm_buffer_pool_used_buffers - jvm_memory_bytes_used - jvm_memory_bytes_committed - jvm_memory_bytes_max - jvm_memory_bytes_init #gc - jvm_gc_collection_seconds #threads - jvm_threads_current - jvm_threads_daemon - jvm_threads_peak - jvm_threads_started_total - jvm_threads_deadlocked - jvm_threads_deadlocked_monitor - jvm_threads_state #classes - jvm_classes_currently_loaded #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

webhcat_fd_thresholds

Required

false

WebHCat Server Host Health Test

Description

When computing the overall WebHCat Server health, consider the host's health.

Related Name

Default Value

true

API Name

webhcat_host_health_enabled

Required

false

WebHCat Server Process Health Test

Description

Enables the health test that the WebHCat Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

webhcat_scm_health_enabled

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

WebHCat Server Port

Description

Port on which WebHCat Server will listen for connections.

Related Name

templeton.port

Default Value

50111

API Name

hive_webhcat_address_port

Required

false

Resource Management

Java Heap Size of WebHCat Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

hive_webhcat_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: WebHCat Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hcatalog_log_dir

Required

true

Suppress Parameter Validation: WebHCat Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_address_port

Required

true

Suppress Parameter Validation: WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_config_safety_valve

Required

true

Suppress Parameter Validation: WebHCat Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_env_safety_valve

Required

true

Suppress Parameter Validation: WebHCat Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_hive_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for WebHCat Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for WebHCat Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_webhcat_java_opts

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: WebHCat Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: WebHCat Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the WebHCat Server Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webhcat_core_site_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_webhcat_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value
false

API Name
role_health_suppression_webhcat_unexpected_exits

Required
true

Hive LLAP Properties in Cloudera Runtime in 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description
The directory where the client configs will be deployed

Related Name

Default Value
/etc/hive

API Name
client_config_root_dir

Required
true

Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description
For advanced use only, a string to be inserted into the client configuration for hive-site.xml.

Related Name

Default Value

API Name
hive_client_config_safety_valve

Required
false

Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description
For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hive-env.sh

Related Name

Default Value

API Name

hive_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

hive_client_java_opts

Required

false

Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server. Consider increasing this if you have tables with a lot of metadata and see timeout errors. Used by most Hive Metastore clients such as Hive CLI and HiveServer2, but not by Impala. Impala has a separately configured timeout.

Related Name

hive.metastore.client.socket.timeout

Default Value

5 minute(s)

API Name

hive_metastore_timeout

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value
INFO

API Name
log_threshold

Required
false

Monitoring

Enable Configuration Change Alerts

Description
When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value
false

API Name
enable_config_alerts

Required
false

Other

Alternatives Priority

Description
The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value
91

API Name
client_config_priority

Required
true

Resource Management

Client Java Heap Size in Bytes

Description
Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value
2 GiB

API Name
hive_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

HiveServer2

Advanced

HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

hive_hs2_env_safety_valve

Required

false

Hive Metastore Connection Retries Count

Description

Number of retries while opening a connection to the Hive Metastore Server

Related Name

hive.metastore.connect.retries

Default Value

10

API Name

hive_metastore_connection_retries

Required

false

Enable Metrics Subsystem

Description

Controls whether the Hive metrics subsystem is enabled for the role.

Related Name

hive.server2.metrics.enabled

Default Value

true

API Name

hive_metrics_enabled

Required

false

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hive/metrics-hivemetastore/metrics.log. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.location

Default Value

API Name

hive_metrics_sample_file_location

Required

false

Metrics Sample File Logging Frequency

Description

The frequency at which the metrics are logged to the sample file. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.frequency

Default Value

30 second(s)

API Name

hive_metrics_sample_logging_frequency

Required

false

Allow User Substitution

Description

Allow alternate user to be specified as part of HiveServer2 open connection request.

Related Name

hive.server2.allow.user.substitution

Default Value

true

API Name

hive_server2_allow_user_substitution

Required

false

HiveServer2 Transport Mode

Description

The server transport mode.

Related Name

hive.server2.transport.mode

Default Value

binary

API Name

hive_server2_transport_mode

Required

false

HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hivellap_hs2_config_safety_valve

Required

false

Hive Downloaded Resources Directory

Description

Local directory where Hive stores jars downloaded for remote file systems (HDFS). If not specified, Hive uses a default location.

Related Name

hive.downloaded.resources.dir

Default Value

API Name

hiveserver2_downloaded_resources_dir

Required

false

Enable Explain Logging

Description

When enabled, HiveServer2 logs EXPLAIN EXTENDED output for every query at INFO log4j level.

Related Name

hive.log.explain.output

Default Value

false

API Name

hiveserver2_enable_explain_output

Required

false

Hive Local Scratch Directory

Description

Local Directory where Hive stores jars and data when performing a MapJoin optimization. If not specified, Hive uses a default location.

Related Name

hive.exec.local.scratchdir

Default Value

API Name

hiveserver2_exec_local_scratchdir

Required

false

Hive HDFS Scratch Directory

Description

Directory in HDFS where Hive writes intermediate data between MapReduce jobs. If not specified, Hive uses a default location.

Related Name

hive.exec.scratchdir

Default Value

API Name

hiveserver2_exec_scratchdir

Required

false

Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

An XML string that will be inserted verbatim into the Fair Scheduler allocations file. This configuration only has effect in CDH 5.8 or later.

Related Name

Default Value

API Name

hiveserver2_fair_scheduler_safety_valve

Required

false

Idle Operation Timeout

Description

Operation will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero. For a positive value, checked for operations in terminal state only (FINISHED, CANCELED, CLOSED, ERROR). For a negative value, checked for all of the operations regardless of state.

Related Name

hive.server2.idle.operation.timeout

Default Value

6 hour(s)

API Name

hiveserver2_idle_operation_timeout

Required

false

Idle Session Timeout

Description

Session will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero or a negative value.

Related Name

hive.server2.idle.session.timeout

Default Value

1 day(s)

API Name

hiveserver2_idle_session_timeout

Required

false

Exclude Live Operations From Session Idle Time

Description

Session will be considered to be idle only if there is no activity, and there is no pending operation. This setting takes effect only if session idle timeout (hive.server2.idle.session.timeout) and checking (hive.server2.session.check.interval) are enabled.

Related Name

hive.server2.idle.session.check.operation

Default Value

true

API Name

hiveserver2_idle_session_timeout_check_operation

Required

false

Java Configuration Options for HiveServer2

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hiveserver2_java_opts

Required

false

Maximum Query String Length for Show Locks

Description

The maximum length allowed for the query string when the SHOW LOCKS EXTENDED command is executed. Important: The query string is truncated at the length set for this property. Setting this property to a large value puts pressure on ZooKeeper and might cause out-of-memory issues.

Related Name

hive.lock.query.string.max.length

Default Value

10000

API Name

hiveserver2_lock_query_string_max_length

Required

false

Max HiveServer2 Threads

Description

Maximum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.max.worker.threads

Default Value

500

API Name

hiveserver2_max_threads

Required

true

Min HiveServer2 Threads

Description

Minimum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.min.worker.threads

Default Value

5

API Name

hiveserver2_min_threads

Required

true

Session Check Interval

Description

The check interval for session/operation timeout, in milliseconds, which can be disabled by setting to zero or a negative value.

Related Name

hive.server2.session.check.interval

Default Value

15 minute(s)

API Name

hiveserver2_session_check_interval

Required

false

HiveServer2 WebUI Max Threads

Description

The max threads for the HiveServer2 WebUI.

Related Name

hive.server2.webui.max.threads

Default Value

50

API Name

hiveserver2_webui_max_threads

Required

false

HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

hs2_core_site_safety_valve

Required

false

HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HiveServer2 Log Directory

Description

Directory where HiveServer2 will place its log files.

Related Name

Default Value

/var/log/hive

API Name

hive_log_dir

Required

false

Enable HiveServer2 Operations Logging

Description

When enabled, HiveServer2 will temporarily save logs associated with ongoing operations. This enables clients like beeline and Hue to request and display logs for a particular ongoing operation. Logs are removed upon completion of operation.

Related Name

hive.server2.logging.operation.enabled

Default Value

true

API Name

hive_server2_logging_operation_enabled

Required

false

HiveServer2 Operations Log Directory

Description

Top level directory where operation logs are temporarily stored if Enable HiveServer2 Operations Logging is true. Logs are stored in session and operation level subdirectories under this location and are removed on completion of operation.

Related Name

hive.server2.logging.operation.log.location

Default Value

/var/log/hive/operation_logs

API Name

hive_server2_logging_operation_log_location

Required

false

HiveServer2 Logging Threshold

Description

The minimum log level for HiveServer2 logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HiveServer2 Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HiveServer2 Max Log Size

Description

The maximum size, in megabytes, per log file for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hive_llap_hs2_downloaded_resources_directory_free_space_absolute_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hive_llap_hs2_downloaded_resources_directory_free_space_percentage_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hive_llap_hs2_exec_local_scratch_directory_free_space_absolute_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hive_llap_hs2_exec_local_scratch_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hiveserver2_fd_thresholds

Required

false

HiveServer2 Host Health Test

Description

When computing the overall HiveServer2 health, consider the host's health.

Related Name

Default Value

true

API Name

hiveserver2_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

hiveserver2_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

hiveserver2_pause_duration_window

Required

false

HiveServer2 Process Health Test

Description

Enables the health test that the HiveServer2's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hiveserver2_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11121

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'metrics<name=(jvm\.pause.*)><>(.*): (\d+)' name: $1_$2 value: $3

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: strict metric_names: #memory - jvm_buffer_pool_used_bytes - jvm_buffer_pool_capacity_bytes - jvm_buffer_pool_used_buffers - jvm_memory_bytes_used - jvm_memory_bytes_committed - jvm_memory_bytes_max - jvm_memory_bytes_init #gc - jvm_gc_collection_seconds #threads - jvm_threads_current - jvm_threads_daemon - jvm_threads_peak - jvm_threads_started_total - jvm_threads_deadlocked - jvm_threads_deadlocked_monitor - jvm_threads_state #classes - jvm_classes_currently_loaded #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes - jvm_pause_extrasleeptime_count

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Restrict Cross Joins (Cartesian Products)

Description

Whether to allow queries with cross joins. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.cartesian.product

Default Value

false

API Name

hive_restrict_cross_joins

Required

false

Restrict LOAD Queries Against Bucketed Tables

Description

Whether to allow LOAD queries against bucketed tables. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.bucketing

Default Value

true

API Name

hive_restrict_load_bucketed_table

Required

false

Restrict Queries with ORDER BY but no LIMIT clause

Description

Whether to allow queries with an ORDER BY clause, but no LIMIT clause. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.orderby.no.limit

Default Value

false

API Name

hive_restrict_orderby_with_no_limit

Required

false

Restrict Partitioned Table Scans with no Partitioned Column Filter

Description

Whether to allow queries that scan a partitioned table but don't filter on the partition column. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.no.partition.filter

Default Value

false

API Name

hive_restrict_partitioned_scans_no_filter

Required

false

Restrict Unsafe Data Type Comparisons

Description

Whether to allow queries that compare bigints to strings or doubles. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.type.safety

Default Value

true

API Name

hive_restrict_unsafe_comparison

Required

false

Support Dynamic Service Discovery

Description

Whether HiveServer2 supports dynamic service discovery for its clients. To support this, each instance of HiveServer2 currently uses ZooKeeper to register itself, when it is brought up. JDBC/ODBC clients should use the ZooKeeper ensemble: hive.zookeeper.quorum in their connection string.

Related Name

hive.server2.support.dynamic.service.discovery

Default Value

true

API Name

hive_server2_support_dynamic_service_discovery

Required

false

Hive Server Zookeeper Namespace

Description

The parent node in ZooKeeper used by HiveServer2 when supporting dynamic service discovery.

Related Name

hive.server2.zookeeper.namespace

Default Value

hiveserver2-interactive

API Name

hive_server2_zookeeper_namespace

Required

false

Default query queues

Description

A list of comma separated values corresponding to YARN queues of the same name. When HiveServer2 is launched in Tez mode, this configuration needs to be set for multiple Tez sessions to run in parallel on the cluster.

Related Name

hive.server2.tez.default.queues

Default Value

llap

API Name

hivellap_default_query_queues

Required

false

hive.prewarm.enabled

Description

Enables container prewarm for Tez

Related Name

hive.prewarm.enabled

Default Value

false

API Name

hivellap_prewarm_enabled

Required

false

Number of Containers Held

Description

Controls the number of containers to prewarm for Tez

Related Name

hive.prewarm.numcontainers

Default Value

2

API Name

hivellap_prewarm_numcontainers

Required

false

Start Tez session at Initialization

Description

This flag is used in HiveServer2 to enable a user to use HiveServer2 without turning on Tez for HiveServer2. The user could potentially want to run queries over Tez without the pool of sessions.

Related Name

hive.server2.tez.initialize.default.sessions

Default Value

true

API Name

hivellap_tez_initialize_default_sessions

Required

false

Allow custom queues

Description

Whether to allow the users of this HS2 to specify custom queues - yes, no (fail if specified), ignore (use the default queues even if a custom one is specified)

Related Name

hive.server2.tez.sessions.custom.queue.allowed

Default Value

ignore

API Name

hivellap_tez_sessions_custom_queue_allowed

Required

false

HiveServer2 Enable Impersonation

Description

HiveServer2 will impersonate the beeline client user when talking to other services such as MapReduce and HDFS.

Related Name

hive.server2.enable.doAs

Default Value

true

API Name

hiveserver2_enable_impersonation

Required

false

HiveServer2 Load Balancer

Description

Address of the load balancer used for HiveServer2 roles, specified in host:port format. If port is not specified, the port used by HiveServer2 is used. Note: Changing this property regenerates Kerberos keytabs for all HiveServer2 roles.

Related Name

Default Value

API Name

hiveserver2_load_balancer

Required

false

Performance

Enable Dynamic Partitions

Description

Whether or not to allow dynamic partitions in DML/DDL.

Related Name

hive.exec.dynamic.partition

Default Value

true

API Name

hive_exec_dynamic_partition

Required

false

Hive Auto Convert Join Noconditional Size

Description

If Hive auto convert join is on, and the sum of the size for n-1 of the tables/partitions for a n-way join is smaller than the specified size, the join is directly converted to a MapJoin (there is no conditional task).

Related Name

hive.auto.convert.join.noconditionaltask.size

Default Value

50 MiB

API Name

hiveserver2_auto_convert_join_noconditionaltask_size

Required

false

Store Intermediate Data on Blobstore

Description

When writing data to a table on a blobstore (such as S3), whether or not the blobstore should be used to store intermediate data during Hive query execution. Setting this to true can degrade performance for queries that spawn multiple MR / Spark jobs, but is useful for queries whose intermediate data cannot fit in the allocated HDFS cluster.

Related Name

hive.blobstore.use.blobstore.as.scratchdir

Default Value

false

API Name

hiveserver2_blobstore_use_blobstore_as_scratchdir

Required

false

Enable Stats Optimization

Description

Enable optimization that checks if a query can be answered using statistics. If so, answers the query using only statistics stored in metastore.

Related Name

hive.compute.query.using.stats

Default Value

true

API Name

hiveserver2_compute_query_using_stats

Required

false

Enable Cost-Based Optimizer for Hive

Description

Enabled the Calcite-based Cost-Based Optimizer for HiveServer2.

Related Name

hive.cbo.enable

Default Value

true

API Name

hiveserver2_enable_cbo

Required

false

Enable MapJoin Optimization

Description

Enable optimization that converts common join into MapJoin based on input file size.

Related Name

hive.auto.convert.join

Default Value

true

API Name

hiveserver2_enable_mapjoin

Required

false

Fetch Task Query Conversion

Description

Some select queries can be converted to a single FETCH task instead of a MapReduce task, minimizing latency. A value of none disables all conversion, minimal converts simple queries such as SELECT * and filter on partition columns, and more converts SELECT queries including FILTERS.

Related Name

hive.fetch.task.conversion

Default Value

more

API Name

hiveserver2_fetch_task_conversion

Required

false

Fetch Task Query Conversion Threshold

Description

Above this size, queries are converted to fetch tasks.

Related Name

hive.fetch.task.conversion.threshold

Default Value

1 GiB

API Name

hiveserver2_fetch_task_conversion_threshold

Required

false

Input Listing Max Threads

Description

Maximum number of threads that Hive uses to list input files. Increasing this value can improve performance when there are a lot of partitions being read, or when running on blobstores.

Related Name

hive.exec.input.listing.max.threads

Default Value

15

API Name

hiveserver2_input_listing_max_threads

Required

false

Maximum ReduceSink Top-K Memory Usage

Description

The maximum percentage of heap to be used for hash in ReduceSink operator for Top-K selection. 0 means the optimization is disabled. Accepted values are between 0 and 1.

Related Name

hive.limit.pushdown.memory.usage

Default Value

0.04

API Name

hiveserver2_limit_pushdown_memory_usage

Required

false

Load Dynamic Partitions Thread Count

Description

Number of threads used to load dynamically generated partitions. Loading requires renaming the file its final location, and updating some metadata about the new partition. Increasing this can improve performance when there are a lot of partitions dynamically generated.

Related Name

hive.load.dynamic.partitions.thread

Default Value

15

API Name

hiveserver2_load_dynamic_partitions_thread_count

Required

false

Enable Map-Side Aggregation

Description

Enable map-side partial aggregation, which cause the mapper to generate fewer rows. This reduces the data to be sorted and distributed to reducers.

Related Name

hive.map.aggr

Default Value

true

API Name

hiveserver2_map_aggr

Required

false

Ratio of Memory Usage for Map-Side Aggregation

Description

Portion of total memory used in map-side partial aggregation. When exceeded, the partially aggregated results will be flushed from the map task to the reducers.

Related Name

hive.map.aggr.hash.percentmemory

Default Value

0.5

API Name

hiveserver2_map_aggr_hash_memory_ratio

Required

false

Enable Merging Small Files - Map-Only Job

Description

Merge small files at the end of a map-only job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapfiles

Default Value

true

API Name

hiveserver2_merge_mapfiles

Required

false

Enable Merging Small Files - Map-Reduce Job

Description

Merge small files at the end of a map-reduce job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapredfiles

Default Value

false

API Name

hiveserver2_merge_mapredfiles

Required

false

Desired File Size After Merging

Description

The desired file size after merging. This should be larger than hive.merge.smallfiles.avgsize.

Related Name

hive.merge.size.per.task

Default Value

256 MiB

API Name

hiveserver2_merge_size_per_task

Required

false

Small File Average Size Merge Threshold

Description

When the average output file size of a job is less than the value of this property, Hive will start an additional map-only job to merge the output files into bigger files. This is only done for map-only jobs if hive.merge.mapfiles is true, for map-reduce jobs if hive.merge.mapredfiles is true, and for Spark jobs if hive.merge.sparkfiles is true.

Related Name

hive.merge.smallfiles.avgsize

Default Value

16 MiB

API Name

hiveserver2_merge_smallfiles_avgsize

Required

false

MSCK Repair Batch Size

Description

Batch size for the msck repair command (recover partitions command). If the value is greater than zero, new partition information will be sent from HiveServer2 to the Metastore in batches, which can potentially improve memory usage in the Metastore and avoid client read timeout exceptions. If this value is 0, all partition information will sent in a single Thrift call.

Related Name

hive.msck.repair.batch.size

Default Value

3000

API Name

hiveserver2_msck_repair_batch_size

Required

false

Move Files Thread Count

Description

The number of threads used by HiveServer2 to move data from the staging directory to another location (typically to the final table location). A separate thread pool of workers of this size is used for each query, which means this configuration can be set on a per-query basis too.

Related Name

hive.mv.files.thread

Default Value

15

API Name

hiveserver2_mv_files_thread

Required

false

Hive Optimize Sorted Merge Bucket Join

Description

Whether to try sorted merge bucket (SMB) join.

Related Name

hive.optimize.bucketmapjoin.sortedmerge

Default Value

false

API Name

hiveserver2_optimize_bucketmapjoin_sortedmerge

Required

false

Enable Automatic Use of Indexes

Description

Whether to use the indexing optimization for all queries.

Related Name

hive.optimize.index.filter

Default Value

true

API Name

hiveserver2_optimize_index_filter

Required

false

Enable ReduceDeDuplication Optimization

Description

Remove extra map-reduce jobs if the data is already clustered by the same key, eliminating the need to repartition the dataset again.

Related Name

hive.optimize.reducededuplication

Default Value

true

API Name

hiveserver2_optimize_reducededuplication

Required

false

Mininum Reducers for ReduceDeDuplication Optimization

Description

When the number of ReduceSink operators after merging is less than this number, the ReduceDeDuplication optimization will be disabled.

Related Name

hive.optimize.reducededuplication.min.reducer

Default Value

4

API Name

hiveserver2_optimize_reducededuplication_min_reducer

Required

false

Enable Sorted Dynamic Partition Optimizer

Description

When dynamic partition is enabled, reducers keep only one record writer at all times, which lowers the memory pressure on reducers.

Related Name

hive.optimize.sort.dynamic.partition

Default Value

false

API Name

hiveserver2_optimize_sort_dynamic_partition

Required

false

Enable Parallel Compilation of Queries

Description

When activated, individual sessions can compile queries simultaneously. Within each session, queries compile one at a time.

Related Name

hive.driver.parallel.compilation

Default Value

true

API Name

hiveserver2_parallel_compilation_enabled

Required

false

Query Compilation Degree of Parallelism

Description

Determines the maximum number of queries that can compile in parallel on a HiveServer2 instance. Use negative values or zero to set unlimited parallelism. Use a positive value to set the number of queries that can compile simultaneously. This setting can be fine-tuned based on the current cluster load. Monitor cluster load using the 'waiting_compile_ops' metric and the 'Waiting Compile Operations' graph in the HiveServer2 graph library.

Related Name

hive.driver.parallel.compilation.global.limit

Default Value

5

API Name

hiveserver2_parallel_compilation_global_limit

Required

false

Hive SMB Join Cache Rows

Description

The number of rows with the same key value to be cached in memory per SMB-joined table.

Related Name

hive.smbjoin.cache.rows

Default Value

10000

API Name

hiveserver2_smbjoin_cache_rows

Required

false

Load Column Statistics

Description

Whether column stats for a table are fetched during explain.

Related Name

hive.stats.fetch.column.stats

Default Value

true

API Name

hiveserver2_stats_fetch_column_stats

Required

false

Sessions Per Queue

Description

The number of Tez sessions that should be launched on each of the queues specified by "hive.server2.tez.default.queues". Determines the parallelism on each queue.

Related Name

hive.server2.tez.sessions.per.default.queue

Default Value

4

API Name

hiveserver2_tez_sessions_per_default_queue

Required

false

Vectorized Adapter Usage Mode

Description

Vectorized Adaptor Usage Mode specifies the extent to which the vectorization engine tries to vectorize UDFs that do not have native vectorized versions available. Selecting the "none" option specifies that only queries using native vectorized UDFs are vectorized. Selecting the "chosen" option specifies that Hive choses to vectorize a subset of the UDFs based on performance benefits using the Vectorized Adaptor. Selecting the "all" option specifies that the Vectorized Adaptor be used for all UDFs even when native vectorized versions are not available.

Related Name

hive.vectorized.adaptor.usage.mode

Default Value

chosen

API Name

hiveserver2_vectorized_adaptor_usage_mode

Required

false

Enable Vectorization Optimization

Description

Enable optimization that vectorizes query execution by streamlining operations by processing a block of 1024 rows at a time.

Related Name

hive.vectorized.execution.enabled

Default Value

true

API Name

hiveserver2_vectorized_enabled

Required

false

Vectorized GroupBy Check Interval

Description

In vectorized group-by, the number of row entries added to the hash table before re-checking average variable size for memory usage estimation.

Related Name

hive.vectorized.groupby.checkinterval

Default Value

4096

API Name

hiveserver2_vectorized_groupby_checkinterval

Required

false

Vectorized GroupBy Flush Ratio

Description

Ratio between 0.0 and 1.0 of entries in the vectorized group-by aggregation hash that is flushed when the memory threshold is exceeded.

Related Name

hive.vectorized.groupby.flush.percent

Default Value

0.1

API Name

hiveserver2_vectorized_groupby_flush_ratio

Required

false

Enable Vectorized Input Format

Description

If enabled, Hive uses the native vectorized input format for vectorized query execution when it is available.

Related Name

hive.vectorized.use.vectorized.input.format

Default Value

true

API Name

hiveserver2_vectorized_input_format_enabled

Required

false

Exclude Vectorized Input Formats

Description

Specifies a list of file input format classnames to exclude from vectorized query execution using the vectorized input format. Note that vectorized execution can still occur for an excluded input format based on whether row SerDes or vector SerDes are enabled.

Related Name

hive.vectorized.input.format.excludes

Default Value

API Name

hiveserver2_vectorized_input_format_excludes

Required

false

Enable Reduce-Side Vectorization

Description

Whether to vectorize the reduce side of query execution.

Related Name

hive.vectorized.execution.reduce.enabled

Default Value

true

API Name

hiveserver2_vectorized_reduce_enabled

Required

false

Enable Overflow-checked Vector Expressions

Description

To enhance performance, vectorized expressions operate using wide data types like long and double. When wide data types are used, numeric overflows can occur during expression evaluation in a different manner for vectorized expressions than they do for non-vectorized expressions. Consequently, different query results can be returned for vectorized expressions compared to results returned for non-vectorized expressions. When this configuration is enabled, Hive uses vectorized expressions that handle numeric overflows in the same way as non-vectorized expressions are handled.

Related Name

hive.vectorized.use.checked.expressions

Default Value

true

API Name

hiveserver2_vectorized_use_checked_expressions

Required

false

Vectorize Using Vector SerDes

Description

If enabled, Hive uses built-in vector SerDes to process text and sequencefile tables for vectorized query execution.

Related Name

hive.vectorized.use.vector.serde.deserialize

Default Value

false

API Name

hiveserver2_vectorized_use_vector_serde_deserialize

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Thrift port

Description

TCP port number to listen on.

Related Name

hive.server2.thrift.http.port

Default Value

10501

API Name

hive_server2_thrift_http_port

Required

false

Bind HiveServer2 to Wildcard Address

Description

If enabled, the HiveServer2 binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

hive.server2.webui.host

Default Value

true

API Name

hiveserver2_webui_bind_wildcard

Required

false

HiveServer2 WebUI Port

Description

The port the HiveServer2 WebUI will listen on. This can be set to 0 to disable the WebUI.

Related Name

hive.server2.webui.port

Default Value

10502

API Name

hiveserver2_webui_port

Required

false

HiveServer2 Port

Description

Port on which HiveServer2 will listen for connections.

Related Name

hive.server2.thrift.port

Default Value

10500

API Name

hs2_thrift_address_port

Required

false

Resource Management

Java Heap Size of HiveServer2 in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

hiveserver2_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

HiveServer2 WebUI SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from WebUI SSL.

Related Name

hive.server2.webui.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_webui_exclude_ciphersuites

Required

false

Enable TLS/SSL for HiveServer2 WebUI

Description

Encrypt communication between clients and HiveServer2 WebUI using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.webui.use.ssl

Default Value

false

API Name

ssl_enabled

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 WebUI is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.webui.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 WebUI keystore file.

Related Name

hive.server2.webui.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Parameter Validation: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Operations Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Parameter Validation: Thrift port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Thrift port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_thrift_http_port

Required

true

Suppress Parameter Validation: Hive Server Zookeeper Namespace

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Server Zookeeper Namespace parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_zookeeper_namespace

Required

true

Suppress Parameter Validation: Default query queues

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default query queues parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_default_query_queues

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_hs2_config_safety_valve

Required

true

Suppress Parameter Validation: Allow custom queues

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allow custom queues parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_tez_sessions_custom_queue_allowed

Required

true

Suppress Parameter Validation: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Downloaded Resources Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Parameter Validation: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Local Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Parameter Validation: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive HDFS Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Parameter Validation: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HiveServer2 parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Parameter Validation: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Parameter Validation: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Vectorized Input Formats parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Parameter Validation: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: tez.history.logging.taskattempt-filters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the tez.history.logging.taskattempt-filters parameter.

Related Name

Default Value

false

API Name

role_config_suppression_tez_interactive_history_logging_taskattempt_filters

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_pause_duration

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hiveserver2_unexpected_exits

Required

true

Suppress Health Test: Hive Downloaded Resources Directory Free Space

Description

Whether to suppress the results of the Hive Downloaded Resources Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hs2_downloaded_resources_directory_free_space

Required

true

Suppress Health Test: Hive Local Scratch Directory Free Space

Description

Whether to suppress the results of the Hive Local Scratch Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_hs2_exec_local_scratch_directory_free_space

Required

true

Tez interactive

tez.am.am-rm.heartbeat.interval-ms.max

Description

The heartbeat interval between the tez AM and YARN RM

Related Name

tez.am.am-rm.heartbeat.interval-ms.max

Default Value

10 second(s)

API Name

tez_interactive_am_am_rm_heartbeat_interval_ms_max

Required

false

tez.am.client.heartbeat.poll.interval.millis

Description

The interval at which the AM checks for a client heartbeat timeout

Related Name

tez.am.client.heartbeat.poll.interval.millis

Default Value

6 second(s)

API Name

tez_interactive_am_client_heartbeat_poll_interval_millis

Required

false

tez.am.client.heartbeat.timeout.secs

Description

The time interval, after which an AM will kill itself, if it does not receive a heartbeat from the client.

Related Name

tez.am.client.heartbeat.timeout.secs

Default Value

1 minute(s), 30 second(s)

API Name

tez_interactive_am_client_heartbeat_timeout_secs

Required

false

tez.am.node-blacklisting.enabled

Description

Whether to enable blacklisting in Tez AMs. Disable for LLAP

Related Name

tez.am.node-blacklisting.enabled

Default Value

false

API Name

tez_interactive_am_node_blacklisting_enabled

Required

false

tez.am.resource.memory.mb

Description

The amount of memory to be used by the AppMaster

Related Name

tez.am.resource.memory.mb

Default Value

1 GiB

API Name

tez_interactive_am_resource_memory_mb

Required

false

tez.am.task.listener.thread-count

Description

Number of IPC server thread for Tez task listener. Should be minimized for LLAP

Related Name

tez.am.task.listener.thread-count

Default Value

1

API Name

tez_interactive_am_task_listener_thread_count

Required

false

tez.am.task.reschedule.higher.priority

Description

Whether rescheduled tasks should be treated at higher priority

Related Name

tez.am.task.reschedule.higher.priority

Default Value

false

API Name

tez_interactive_am_task_reschedule_higher_priority

Required

false

tez.container.max.java.heap.fraction

Description

Setting this to -1 so that Tez can auto determine different Xmx for different container size

Related Name

tez.container.max.java.heap.fraction

Default Value

-1.0

API Name

tez_interactive_container_max_java_heap_fraction

Required

false

tez.dag.recovery.enabled

Description

tez.dag.recovery.enabled

Related Name

tez.dag.recovery.enabled

Default Value

false

API Name

tez_interactive_dag_recovery_enabled

Required

false

tez.grouping.node.local.only

Description

tez.grouping.node.local.only

Related Name

tez.grouping.node.local.only

Default Value

true

API Name

tez_interactive_grouping_node_local_only

Required

false

tez.history.logging.log.level

Description

Set the log level to TASK_ATTEMPT.

Related Name

tez.history.logging.log.level

Default Value

TASK_ATTEMPT

API Name

tez_interactive_history_logging_log_level

Required

false

tez.history.logging.taskattempt-filters

Description

TASK_ATTEMPT events to be ignored.

Related Name

tez.history.logging.taskattempt-filters

Default Value

SERVICE_BUSY, EXTERNAL_PREEMPTION

API Name

tez_interactive_history_logging_taskattempt_filters

Required

false

tez.history.logging.timeline.num-dags-per-group

Description

Maximum number of dags per group.

Related Name

tez.history.logging.timeline.num-dags-per-group

Default Value

5

API Name

tez_interactive_history_logging_timeline_num_dags_per_group

Required

false

tez.runtime.enable.final-merge.in.output

Description

Whether to enable a map side merge of outputs

Related Name

tez.runtime.enable.final-merge.in.output

Default Value

false

API Name

tez_interactive_runtime_enable_final_merge_in_output

Required

false

tez.runtime.io.sort.mb

Description

The size of the sort buffer when output needs to be sorted

Related Name

tez.runtime.io.sort.mb

Default Value

512 MiB

API Name

tez_interactive_runtime_io_sort_mb

Required

false

tez.runtime.pipelined-shuffle.enabled

Description

tez.runtime.pipelined-shuffle.enabled

Related Name

tez.runtime.pipelined-shuffle.enabled

Default Value

false

API Name

tez_interactive_runtime_pipelined_shuffle_enabled

Required

false

tez.runtime.pipelined.sorter.lazy-allocate.memory

Description

tez.runtime.pipelined.sorter.lazy-allocate.memory

Related Name

tez.runtime.pipelined.sorter.lazy-allocate.memory

Default Value

true

API Name

tez_interactive_runtime_pipelined_sorter_lazy_allocate_memory

Required

false

tez.runtime.report.partition.stats

Description

tez.runtime.report.partition.stats

Related Name

tez.runtime.report.partition.stats

Default Value

true

API Name

tez_interactive_runtime_report_partition_stats

Required

false

tez.runtime.shuffle.connect.timeout

Description

Shuffle connect timeouts (ms)

Related Name

tez.runtime.shuffle.connect.timeout

Default Value

30 second(s)

API Name

tez_interactive_runtime_shuffle_connect_timeout

Required

false

tez.runtime.shuffle.fetch.buffer.percent

Description

Fraction (0-1) of the available memory which can be used to retain shuffled data

Related Name

tez.runtime.shuffle.fetch.buffer.percent

Default Value

0.6

API Name

tez_interactive_runtime_shuffle_fetch_buffer_percent

Required

false

tez.runtime.shuffle.fetch.verify-disk-checksum

Description

tez.runtime.shuffle.fetch.verify-disk-checksum

Related Name

tez.runtime.shuffle.fetch.verify-disk-checksum

Default Value

false

API Name

tez_interactive_runtime_shuffle_fetch_verify_disk_checksum

Required

false

tez.runtime.shuffle.keep-alive.enabled

Description

Connection keep-alive for shuffle

Related Name

tez.runtime.shuffle.keep-alive.enabled

Default Value

true

API Name

tez_interactive_runtime_shuffle_keep_alive_enabled

Required

false

tez.runtime.shuffle.memory.limit.percent

Description

This property determines the maximum size of a shuffle segment which can be fetched to memory. Fraction (0-1) of shuffle memory (after applying tez.runtime.shuffle.fetch.buffer.percent)

Related Name

tez.runtime.shuffle.memory.limit.percent

Default Value

0.25

API Name

tez_interactive_runtime_shuffle_memory_limit_percent

Required

false

tez.runtime.shuffle.parallel.copies

Description

tez.runtime.shuffle.parallel.copies

Related Name

tez.runtime.shuffle.parallel.copies

Default Value

8

API Name

tez_interactive_runtime_shuffle_parallel_copies

Required

false

tez.runtime.shuffle.read.timeout

Description

Shuffle read timeout (ms)

Related Name

tez.runtime.shuffle.read.timeout

Default Value

30 second(s)

API Name

tez_interactive_runtime_shuffle_read_timeout

Required

false

tez.runtime.shuffle.ssl.enable

Description

tez.runtime.shuffle.ssl.enable

Related Name

tez.runtime.shuffle.ssl.enable

Default Value

false

API Name

tez_interactive_runtime_shuffle_ssl_enable

Required

false

tez.runtime.unordered.output.buffer.size-mb

Description

The size of the buffer when output does not require to be sorted

Related Name

tez.runtime.unordered.output.buffer.size-mb

Default Value

100 MiB

API Name

tez_interactive_runtime_unordered_output_buffer_size_mb

Required

false

tez.runtime.unordered.output.max-per-buffer.size-bytes

Description

tez.runtime.unordered.output.max-per-buffer.size-bytes

Related Name

tez.runtime.unordered.output.max-per-buffer.size-bytes

Default Value

128 MiB

API Name

tez_interactive_runtime_unordered_output_max_per_buffer_size_bytes

Required

false

tez.session.am.dag.submit.timeout.secs

Description

The amount of time an AM will wait, before killing itself, if not DAG is submitted.

Related Name

tez.session.am.dag.submit.timeout.secs

Default Value

14 day(s)

API Name

tez_interactive_session_am_dag_submit_timeout_secs

Required

false

tez.task.heartbeat.timeout.check-ms

Description

The time interval, in milliseconds, at which the AM will check for timed out tasks

Related Name

tez.task.heartbeat.timeout.check-ms

Default Value

15 second(s)

API Name

tez_interactive_task_heartbeat_timeout_check_ms

Required

false

tez.task.timeout-ms

Description

mount of time the Tez AM waits before marking a task which has not sent in a heartbeat, as timed out

Related Name

tez.task.timeout-ms

Default Value

1 minute(s), 30 second(s)

API Name

tez_interactive_task_timeout_ms

Required

false

LLAP Proxy

Advanced

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hive/metrics-hivemetastore/metrics.log. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.location

Default Value

API Name

hive_metrics_sample_file_location

Required

false

LLAP Daemon Java Options

Description

Extra Java options that will be applied on the JVM processes of LLAP Daemons.

Related Name

Default Value

API Name

hivellap_daemon_opts

Required

false

LLAP Proxy Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hivellap_llapproxy_config_safety_valve

Required

false

LLAP Proxy Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

LLAPPROXY_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

LLAP Proxy Log Directory

Description

Directory where LLAP Proxy will place its log files.

Related Name

Default Value

/var/log/hive

API Name

hive_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Hive LLAP Daemons Ready Status Startup Tolerance

Description

Bad health state will be shown if, after this amount of time (after starting LLAP proxy role), 0 LLAP daemons are running.

Related Name

Default Value

5 minute(s)

API Name

llapd_ready_status_check_daemon_startup_tolerance

Required

false

Hive LLAP Proxy Role Ready Status Startup Tolerance

Description

Startup Tolerance time of the LLAP proxy role in which no health test is run. This is recommended to be kept minimal.

Related Name

Default Value

1 second(s)

API Name

llapd_ready_status_check_role_startup_tolerance

Required

false

Hive LLAP Daemons Ready Status Thresholds

Description

The health test thresholds for monitoring the number of active LLAP daemons.

Related Name

Default Value

Warning: 75.0, Critical: 25.0

API Name

llapd_ready_status_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

llapproxy_fd_thresholds

Required

false

LLAP Proxy Host Health Test

Description

When computing the overall LLAP Proxy health, consider the host's health.

Related Name

Default Value

true

API Name

llapproxy_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

llapproxy_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

llapproxy_pause_duration_window

Required

false

LLAP Proxy Process Health Test

Description

Enables the health test that the LLAP Proxy's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

llapproxy_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

hive.llap.auto.allow.uber

Description

Whether or not to allow the planner to run vertices in the AM

Related Name

hive.llap.auto.allow.uber

Default Value

false

API Name

hivellap_auto_allow_uber

Required

false

In-Memory Cache per Daemon

Description

The amount of memory reserved for Hive's optimized in-memory cache.

Related Name

hive.llap.io.memory.size

Default Value

512 MiB

API Name

hivellap_cache_per_llap_daemon

Required

false

hive.llap.client.consistent.splits

Description

Whether to setup split locations to match nodes on which llap daemons are running, instead of using the locations provided by the split itself.

Related Name

hive.llap.client.consistent.splits

Default Value

true

API Name

hivellap_client_consistent_splits

Required

false

hive.llap.daemon.am.liveness.heartbeat.interval.ms

Description

Tez AM-LLAP heartbeat interval. This should be below the task timeout.

Related Name

hive.llap.daemon.am.liveness.heartbeat.interval.ms

Default Value

10 second(s)

API Name

hivellap_daemon_am_heartbeat_interval

Required

false

Number of nodes used by Hive's LLAP

Description

Number of nodes used by Hive's LLAP, which includes LLAP nodes running. Yarn native service container and Tez App Master(s) are not part of this.

Related Name

num_llap_nodes

Default Value

1

API Name

hivellap_daemon_count

Required

false

hive.llap.daemon.logger

Description

Logger to be used by LLAP. (query-routing, RFA)

Related Name

hive.llap.daemon.logger

Default Value

llap

API Name

hivellap_daemon_logger

Required

false

hive.llap.daemon.rpc.port

Description

The LLAP daemon RPC port.

Related Name

hive.llap.daemon.rpc.port

Default Value

0

API Name

hivellap_daemon_rpc_port

Required

false

hive.llap.daemon.task.scheduler.enable.preemption

Description

hive.llap.daemon.task.scheduler.enable.preemption

Related Name

hive.llap.daemon.task.scheduler.enable.preemption

Default Value

true

API Name

hivellap_daemon_task_scheduler_enable_preemption

Required

false

hive.llap.daemon.vcpus.per.instance

Description

The total number of vcpus to use for the executors inside LLAP.

Related Name

hive.llap.daemon.vcpus.per.instance

Default Value

0

API Name

hivellap_daemon_vcpus_per_instance

Required

false

hive.llap.daemon.yarn.shuffle.port

Description

YARN shuffle port for LLAP-daemon-hosted shuffle.

Related Name

hive.llap.daemon.yarn.shuffle.port

Default Value

15551

API Name

hivellap_daemon_yarn_shuffle_port

Required

false

dfs.client.mmap.enabled

Description

Disable HDFS caching fo LLAP

Related Name

dfs.client.mmap.enabled

Default Value

false

API Name

hivellap_dfs_client_mmap_enabled

Required

false

dfs.short.circuit.shared.memory.watcher.interrupt.check.ms

Description

Disable HDFS caching fo LLAP

Related Name

dfs.short.circuit.shared.memory.watcher.interrupt.check.ms

Default Value

0 second(s)

API Name

hivellap_dfs_shared_mem_watcher_interrupt

Required

false

hive.llap.enable.grace.join.in.llap

Description

Override if grace join should be allowed to run in llap for regular map joins. Dynamic partitioned joins will honor the hive.mapjoin.hybridgrace.hashtable property in LLAP

Related Name

hive.llap.enable.grace.join.in.llap

Default Value

false

API Name

hivellap_enable_grace_join_in_llap

Required

false

hive.execution.mode

Description

Chooses whether query fragments will run in container or in llap

Related Name

hive.execution.mode

Default Value

llap

API Name

hivellap_execution_mode

Required

false

Number of executors per LLAP Daemon

Description

The number of fragments that a single LLAP daemon will run concurrently. Usually, this will be the same as the number of available CPUs

Related Name

hive.llap.daemon.num.executors

Default Value

2

API Name

hivellap_executors_per_llap_daemon

Required

false

LLAP Daemon Heap Size in MB.

Description

LLAP Daemon Heap Size in MB.

Related Name

llap_heap_size

Default Value

1280 MiB

API Name

hivellap_heap_per_llap_daemon

Required

false

hive.llap.io.enabled

Description

Whether the LLAP IO layer is enabled.

Related Name

hive.llap.io.enabled

Default Value

true

API Name

hivellap_io_enabled

Required

false

hive.llap.io.memory.mode

Description

LLAP IO memory usage; 'cache' (the default) uses data and metadata cache with a custom off-heap allocator, 'allocator' uses the custom allocator without the caches, 'none' doesn't use either (this mode may result in significant performance degradation)

Related Name

hive.llap.io.memory.mode

Default Value

cache

API Name

hivellap_io_memory_mode

Required

false

hive.llap.io.threadpool.size

Description

Specify the number of threads to use for low-level IO thread pool.

Related Name

hive.llap.io.threadpool.size

Default Value

2

API Name

hivellap_io_threadpool_size

Required

false

hive.llap.io.use.lrfu

Description

Whether ORC low-level cache should use LRFU cache policy instead of default (FIFO).

Related Name

hive.llap.io.use.lrfu

Default Value

true

API Name

hivellap_io_use_lrfu

Required

false

hive.llap.execution.mode

Description

Chooses which fragments of a query will run in llap

Related Name

hive.llap.execution.mode

Default Value

only

API Name

hivellap_llap_execution_mode

Required

false

hive.llap.management.rpc.port

Description

RPC port for LLAP daemon management service.

Related Name

hive.llap.management.rpc.port

Default Value

15004

API Name

hivellap_management_rpc_port

Required

false

hive.llap.mapjoin.memory.oversubscribe.factor

Description

hive.llap.mapjoin.memory.oversubscribe.factor

Related Name

hive.llap.mapjoin.memory.oversubscribe.factor

Default Value

0.3

API Name

hivellap_mapjoin_memory_oversubscribe_factor

Required

false

Maximum Total Concurrent Queries

Description

The maximum number of queries the Hive Interactive cluster will be able to handle concurrently.

Related Name

hive.server2.tez.sessions.per.default.queue

Default Value

1

API Name

hivellap_max_total_concurrent_queries

Required

false

Memory per Daemon

Description

Total memory used by individual LLAP daemons (YARN Container size). This includes memory for the cache as well as for the query execution. Should be larger than the sum of the Daemon cache size and the daemon heap size, and should leave some headroom after this (In most cases: cache size + heap size + headroom = Memory Per Daemon).

Related Name

hive.llap.daemon.yarn.container.mb

Default Value

2 GiB

API Name

hivellap_memory_per_llap_daemon

Required

false

hive.llap.object.cache.enabled

Description

Cache objects (plans, hashtables, etc) in llap.

Related Name

hive.llap.object.cache.enabled

Default Value

true

API Name

hivellap_object_cache_enabled

Required

false

Interactive Query Queue

Description

Choose the YARN queue in this cluster that is dedicated to interactive query.

Related Name

hive.llap.daemon.queue.name

Default Value

llap

API Name

hivellap_queue_name

Required

false

llap.shuffle.connection-keep-alive.enable

Description

llap.shuffle.connection-keep-alive.enable

Related Name

llap.shuffle.connection-keep-alive.enable

Default Value

true

API Name

hivellap_shuffle_connection_keep_alive_enable

Required

false

llap.shuffle.connection-keep-alive.timeout

Description

llap.shuffle.connection-keep-alive.timeout

Related Name

llap.shuffle.connection-keep-alive.timeout

Default Value

1 minute(s)

API Name

hivellap_shuffle_connection_keep_alive_timeout

Required

false

Turn SSD Cache On?

Description

Turn SSD Cache On?

Related Name

hive.llap.io.allocator.mmap

Default Value

false

API Name

hivellap_ssd_cache_on

Required

false

hive.llap.task.scheduler.locality.delay

Description

Amount of time to wait before allocating a request which contains location information, to a location other than the ones requested. Set to -1 for an infinite delay, 0 for no delay.

Related Name

hive.llap.task.scheduler.locality.delay

Default Value

1

API Name

hivellap_task_scheduler_locality_delay

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: LLAP Proxy Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LLAP Proxy Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Parameter Validation: hive.llap.daemon.logger

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the hive.llap.daemon.logger parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_daemon_logger

Required

true

Suppress Parameter Validation: LLAP Daemon Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LLAP Daemon Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_daemon_opts

Required

true

Suppress Parameter Validation: hive.execution.mode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the hive.execution.mode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_execution_mode

Required

true

Suppress Parameter Validation: hive.llap.io.memory.mode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the hive.llap.io.memory.mode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_io_memory_mode

Required

true

Suppress Parameter Validation: hive.llap.execution.mode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the hive.llap.execution.mode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_llap_execution_mode

Required

true

Suppress Parameter Validation: LLAP Proxy Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LLAP Proxy Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_llapproxy_config_safety_valve

Required

true

Suppress Parameter Validation: Interactive Query Queue

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Interactive Query Queue parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_queue_name

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: LLAP Proxy Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LLAP Proxy Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_llapproxy_role_env_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_pause_duration

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_llap_llapproxy_unexpected_exits

Required

true

Suppress Health Test: LLAP Daemons Ready Check

Description

Whether to suppress the results of the LLAP Daemons Ready Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_llapd_ready_status

Required

true

Service-Wide

Advanced

Hive Auxiliary JARs Directory

Description

Directory containing auxiliary JARs used by Hive. This should be a directory location and not a classpath containing one or more JARs. This directory must be created and managed manually on hosts that run the Hive Metastore Server, HiveServer2, or the Hive CLI. The directory location is set in the environment as HIVE_AUX_JARS_PATH and will generally override the hive.aux.jars.path property set in XML files, even if hive.aux.jars.path is set in an advanced configuration snippet.

Related Name

Default Value

API Name

hive_aux_jars_path_dir

Required

false

Bypass Hive Metastore Server

Description

Instead of talking to Hive Metastore Server for Metastore information, Hive clients will talk directly to the Metastore database.

Related Name

Default Value

false

API Name

hive_bypass_metastore_server

Required

false

Aborted Transaction Threshold

Description

Number of aborted transactions involving a particular table or partition before major compaction is initiated.

Related Name

hive.compactor.abortedtxn.threshold

Default Value

1000

API Name

hive_compactor_abortedtxn_threshold

Required

true

Number of Threads Used by Compactor

Description

Number of compactor worker threads to run on this metastore instance. Can be different values on different Metastore instances.

Related Name

hive.compactor.worker.threads

Default Value

5

API Name

hive_compactor_worker_threads

Required

true

Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_core_site_safety_valve

Required

false

Default Table Format - Create Tables as Full ACID

Description

Whether the eligible tables should be created as full ACID by default. Does not apply to external tables, the ones using storage handlers, etc.

Related Name

hive.create.as.acid

Default Value

true

API Name

hive_create_as_acid

Required

false

Default Table Format - Create Tables as ACID Insert Only

Description

Whether the eligible tables should be created as ACID insert-only by default. Does not apply to external tables, the ones using storage handlers, etc.

Related Name

hive.create.as.insert.only

Default Value

true

API Name

hive_create_as_insert_only

Required

false

Hive Copy Large File Size

Description

Smaller than this size, Hive uses a single-threaded copy; larger than this size, Hive uses DistCp.

Related Name

hive.exec.copyfile.maxsize

Default Value

32 MiB

API Name

hive_exec_copyfile_maxsize

Required

false

Base Directory for Hive Proto Hook

Description

The directory where hive proto hooks should write the events, should generally be location of query_data table under sys.db database.

Related Name

hive.hook.proto.base-directory

Default Value

/warehouse/tablespace/managed/hive/sys.db/query_data/

API Name

hive_hook_proto_base_directory

Required

false

Hive LLAP Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

HIVE_LLAP_service_env_safety_valve

Required

false

Metastore Transactional Listener List

Description

A comma separated list of Java classes that implement the org.apache.hadoop.hive.metastore.MetaStoreEventListener interface. Both the metastore event and corresponding listener method will be invoked in the same JDO transaction.

Related Name

hive.metastore.transactional.event.listeners

Default Value

org.apache.hive.hcatalog.listener.DbNotificationListener

API Name

hive_metastore_transactional_event_listeners

Required

false

Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the environment of Hive replication jobs.

Related Name

Default Value

API Name

hive_replication_env_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_service_config_safety_valve

Required

false

Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to all Hive Replication jobs.

Related Name

Default Value

API Name

hive_service_replication_config_safety_valve

Required

false

Use Locking

Description

Support concurrency and use locks, needed for Transactions. Requires Zookeeper.

Related Name

hive.support.concurrency

Default Value

true

API Name

hive_support_concurrency

Required

false

Transaction Manager

Description

HiveTxnManager implementation used for managing transactions.

Related Name

hive.txn.manager

Default Value

org.apache.hadoop.hive.ql.lockmgr.DbTxnManager

API Name

hive_txn_manager

Required

true

Transaction Maximum Open Batch

Description

Maximum number of transactions that can be fetched in one call to open_txns(). Increasing this will decrease the number of delta files created when streaming data into Hive. But it will also increase the number of open transactions at any given time, possibly impacting read performance.

Related Name

hive.txn.max.open.batch

Default Value

1000

API Name

hive_txn_max_open_batch

Required

true

Transaction Strict Locking Mode

Description

In strict locking non-ACID resources use standard R/W lock semantics.

Related Name

hive.txn.strict.locking.mode

Default Value

false

API Name

hive_txn_strict_locking_mode

Required

false

Transaction Timeout

Description

Time after which transactions are declared aborted if the client has not sent a heartbeat.

Related Name

hive.txn.timeout

Default Value

5 minute(s)

API Name

hive_txn_timeout

Required

true

Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.lineage.client.properties.

Related Name

Default Value

API Name

navigator_lineage_client_config_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_username

Required

true

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

For advanced use only, a string to be inserted into ranger-hive-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-hive-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

For advanced use only, a string to be inserted into ranger-hive-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for Hive events:

- userName: the user performing the action.
- ipAddress: the IP from where the request originated.
- operation: the Hive operation being performed.
- databaseName: the databaseName for the operation.
- tableName: the tableName for the operation.

The default Hive audit event filter discards HDFS directory events generated by Hive jobs that reference the /tmp directory.

Related Name

navigator.event.filter

Default Value

comment: [The default Hive audit event filter discards HDFS directory events , generated by Hive jobs that reference the /tmp directory.], defaultAction: accept, rules: [action: discard, fields: [name: operation, match: QUERY , name: objectType, match: DFS_DIR , name: resourcePath, match: /tmp/hive-(?:.+)?/hive_(?:.+)?/-mr-.*]]

API Name

navigator_audit_event_filter

Required

false

Audit Queue Policy

Description

Action to take when the audit event queue is full. Drop the event or shutdown the affected process.

Related Name

navigator.batch.queue_policy

Default Value

DROP

API Name

navigator_audit_queue_policy

Required

false

Audit Event Tracker

Description

Configures the rules for event tracking and coalescing. This feature is used to define equivalency between different audit events. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the "tracked" events according to the rules defined here. Event trackers are defined in a JSON object like the following: { "timeToLive" : [integer], "fields" : [{ "type" : [string], "name" : [string] }] } Where:

- timeToLive: maximum amount of time an event will be tracked, in milliseconds. Must be provided. This defines how long, since it's first seen, an event will be tracked. A value of 0 disables tracking.
- fields: list of fields to compare when matching events against tracked events.

Each field has an evaluator type associated with it. The evaluator defines how the field data is to be compared. The following evaluators are available:

- value: uses the field value for comparison.
- userName: treats the field value as a userNname, and ignores any host-specific data. This is useful for environment using Kerberos, so that only the principal name and realm are compared.

The following is the list of fields that can be used to compare Hive events:

- operation: the Hive operation being performed.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- databaseName: the database affected by the operation.
- tableName: the table or view affected by the operation.
- objectType: the type of object affected by the operation.
- resourcePath: the path of the resource affected by the operation.

Related Name

navigator_event_tracker

Default Value

API Name

navigator_event_tracker

Required

false

Enable Lineage Collection

Description

Enable collection of lineage from the service's roles.

Related Name

Default Value

true

API Name

navigator_lineage_enabled

Required

false

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/hive/audit

API Name

audit_event_log_dir

Required

false

Hive Lineage Log Directory

Description

The directory in which Hive lineage log files are written.

Related Name

lineage_event_log_dir

Default Value

/var/log/hive/lineage

API Name

lineage_event_log_dir

Required

true

Hive Maximum Lineage Log File Size

Description

The maximum size, in megabytes, per log file for Hive lineage logs. Typically used by log4j or logback.

Related Name

max_lineage_log_file_size

Default Value

100 MiB

API Name

max_lineage_log_file_size

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Number of Audit Logs to Retain

Description

Maximum number of rolled-over audit logs to retain. The logs are not deleted if they contain audit events that have not yet been propagated to the Audit Server.

Related Name

navigator.client.max_num_audit_log

Default Value

10

API Name

navigator_client_max_num_audit_log

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hive_llap_hiveserver2s_healthy_thresholds

Required

false

LLAP Proxy Role Health Test

Description

When computing the overall HIVE_LLAP health, consider LLAP Proxy's health

Related Name

Default Value

true

API Name

hive_llap_llapproxy_health_enabled

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "I

F (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", " streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>hive.metastore.client.socket.timeout</name> <value>60</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HBase Service

Description

Name of the HBase service that this Hive service instance depends on.

Related Name

Default Value

API Name

hbase_service

Required

false

HDFS Service

Description

Name of the HDFS service that this Hive service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Enable Asynchronous Logging

Description

Asynchronous Log4j2 logging can give a significant performance improvement as logging will be handled in a separate thread that uses an LMAX disruptor queue for buffering log messages. Refer to https://logging.apache.org/log4j/2.x/manual/async.html for benefits and drawbacks. For debugging issues we recommend setting this to false.

Related Name

hive.async.log.enabled

Default Value

false

API Name

hive_async_log_enabled

Required

false

Hive Bytes Per Reducer

Description

Size per reducer. If the input size is 10GiB and this is set to 1GiB, Hive will use 10 reducers.

Related Name

hive.exec.reducers.bytes.per.reducer

Default Value

64 MiB

API Name

hive_bytes_per_reducer

Required

false

Default File Format

Description

Default file format for CREATE TABLE statement.

Related Name

hive.default.fileformat

Default Value

TextFile

API Name

hive_default_fileformat

Required

true

Default File Format for Managed Tables

Description

Default file format for CREATE TABLE statement applied to managed tables only. External tables will be created with default file format. Leaving this null will result in using the default file format for all tables.

Related Name

hive.default.fileformat.managed

Default Value

ORC

API Name

hive_default_fileformat_managed

Required

false

Hive Max Reducers

Description

Max number of reducers to use. If the configuration parameter Hive Reduce Tasks is negative, Hive will limit the number of reducers to the value of this parameter.

Related Name

hive.exec.reducers.max

Default Value

1009

API Name

hive_max_reducers

Required

false

Hive Reduce Tasks

Description

Default number of reduce tasks per job. Usually set to a prime number close to the number of available hosts. Ignored when mapred.job.tracker is "local". Hadoop sets this to 1 by default, while Hive uses -1 as the default. When set to -1, Hive will automatically determine an appropriate number of reducers for each job.

Related Name

mapred.reduce.tasks

Default Value

-1

API Name

hive_reduce_tasks

Required

false

Set User and Group Information

Description

In unsecure mode, setting this property to true will cause the Metastore Server to execute DFS operations using the client's reported user and group permissions. Cloudera Manager will set this for all clients and servers.

Related Name

hive.metastore.execute.setugi

Default Value

true

API Name

hive_set_ugi

Required

true

LLAP app name

Description

LLAP app name

Related Name

llap_app_name

Default Value

llap0

API Name

hivellap_app_name

Required

false

hive.llap.daemon.service.hosts

Description

Explicitly specified hosts to use for LLAP scheduling. If it's left empty, LLAP app name will be used instead with a ZooKeeper based registry.

Related Name

hive.llap.daemon.service.hosts

Default Value

API Name

hivellap_daemon_service_hosts

Required

false

Hive Metastore Connector

Description

Name of the Hive Metastore Connector from the data context that this service instance depends on.

Related Name

Default Value

API Name

hms_connector

Required

true

MapReduce Service

Description

MapReduce jobs are run against this service.

Related Name

Default Value

API Name

mapreduce_yarn_service

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hive.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hive.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Hive service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Tez Service

Description

Tez Service that the Hive on Tez uses for execution

Related Name

Default Value

API Name

tez_service

Required

true

ZooKeeper Service

Description

Name of the ZooKeeper service that this Hive service instance depends on.

Related Name

Default Value

API Name

zookeeper_service

Required

false

Proxy

Hive Metastore Access Control and Proxy User Groups Override

Description

This configuration overrides the value set for Hive Proxy User Groups configuration in HDFS service for use by Hive Metastore Server. Specify a comma-delimited list of groups that you want to allow access to Hive Metastore metadata and allow the Hive user to impersonate. A value of '*' allows all groups. The default value of empty inherits the value set for Hive Proxy User Groups configuration in the HDFS service.

Related Name

hadoop.proxyuser.hive.groups

Default Value

API Name

hive_proxy_user_groups_list

Required

false

Replication

Replica functions root directory

Description

Root directory on the replica warehouse where the repl sub-system will store jars from the primary warehouse

Related Name

hive.repl.replica.functions.root.dir

Default Value

API Name

hive_repl_replica_functions_root_dir

Required

false

Security

Enable LDAP Authentication for HiveServer2

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

Default Value

false

API Name

hiveserver2_enable_ldap_auth

Required

false

Enable TLS/SSL for HiveServer2

Description

Encrypt communication between clients and HiveServer2 using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.use.SSL

Default Value

false

API Name

hiveserver2_enable_ssl

Required

false

HiveServer2 SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from Hiveserver2 SSL.

Related Name

hive.server2.http.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_exclude_ciphersuites

Required

false

HiveServer2 SSL Include Cipher Suites

Description

The cipher suites should be included in Hiverserver2 SSL.

Related Name

hive.server2.binary.include.ciphersuites

Default Value

modern2018

API Name

hiveserver2_include_ciphersuites

Required

false

HiveServer2 TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 keystore file.

Related Name

hive.server2.keystore.password

Default Value

API Name

hiveserver2_keystore_password

Required

false

HiveServer2 TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.keystore.path

Default Value

API Name

hiveserver2_keystore_path

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like "uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

hive.server2.authentication.ldap.baseDN

Default Value

API Name

hiveserver2_ldap_basedn

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

hive.server2.authentication.ldap.Domain

Default Value

API Name

hiveserver2_ldap_domain

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

hive.server2.authentication.ldap.url

Default Value

API Name

hiveserver2_ldap_uri

Required

false

HiveServer2 TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HiveServer2 might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

hiveserver2_truststore_file

Required

false

HiveServer2 TLS/SSL Trust Store Password

Description

The password for the HiveServer2 TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

hiveserver2_truststore_password

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hive

API Name

kerberos_princ_name

Required

true

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hive

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hive/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hive/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hive.policy.cache.dir

Default Value

/var/lib/ranger/hive/policy-cache

API Name

ranger_policy_cache_dir

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Configuration Validator: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Log Directory

Description

Whether to suppress configuration warnings produced by the HiveServer2 Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Configuration Validator: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the Metrics Sample File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Configuration Validator: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the HiveServer2 Operations Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Configuration Validator: Thrift port

Description

Whether to suppress configuration warnings produced by the Thrift port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_thrift_http_port

Required

true

Suppress Configuration Validator: Hive Server Zookeeper Namespace

Description

Whether to suppress configuration warnings produced by the Hive Server Zookeeper Namespace configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_zookeeper_namespace

Required

true

Suppress Configuration Validator: hive.llap.daemon.logger

Description

Whether to suppress configuration warnings produced by the hive.llap.daemon.logger configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_daemon_logger

Required

true

Suppress Configuration Validator: LLAP Daemon Java Options

Description

Whether to suppress configuration warnings produced by the LLAP Daemon Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_daemon_opts

Required

true

Suppress Configuration Validator: Default query queues

Description

Whether to suppress configuration warnings produced by the Default query queues configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_default_query_queues

Required

true

Suppress Configuration Validator: hive.execution.mode

Description

Whether to suppress configuration warnings produced by the hive.execution.mode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_execution_mode

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_hs2_config_safety_valve

Required

true

Suppress Configuration Validator: hive.llap.io.memory.mode

Description

Whether to suppress configuration warnings produced by the hive.llap.io.memory.mode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_io_memory_mode

Required

true

Suppress Configuration Validator: hive.llap.execution.mode

Description

Whether to suppress configuration warnings produced by the hive.llap.execution.mode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_llap_execution_mode

Required

true

Suppress Configuration Validator: LLAP Proxy Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the LLAP Proxy Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_llapproxy_config_safety_valve

Required

true

Suppress Configuration Validator: Interactive Query Queue

Description

Whether to suppress configuration warnings produced by the Interactive Query Queue configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_queue_name

Required

true

Suppress Configuration Validator: Allow custom queues

Description

Whether to suppress configuration warnings produced by the Allow custom queues configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hivellap_tez_sessions_custom_queue_allowed

Required

true

Suppress Configuration Validator: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the Hive Downloaded Resources Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Configuration Validator: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive Local Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Configuration Validator: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive HDFS Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Configuration Validator: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HiveServer2 configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Configuration Validator: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the HiveServer2 Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Configuration Validator: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the Exclude Vectorized Input Formats configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Configuration Validator: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: LLAP Proxy Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the LLAP Proxy Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_llapproxy_role_env_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HiveServer2 Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: tez.history.logging.taskattempt-filters

Description

Whether to suppress configuration warnings produced by the tez.history.logging.taskattempt-filters configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_tez_interactive_history_logging_taskattempt_filters

Required

true

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Hive Auxiliary JARs Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Auxiliary JARs Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_aux_jars_path_dir

Required

true

Suppress Configuration Validator: Client TLS/SSL In Use With LDAP Authentication Validator

Description

Whether to suppress configuration warnings produced by the Client TLS/SSL In Use With LDAP Authentication Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_client_ssl_recommended_with_ldap_auth_validator

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_core_site_safety_valve

Required

true

Suppress Parameter Validation: Default File Format for Managed Tables

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default File Format for Managed Tables parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_default_fileformat_managed

Required

true

Suppress Parameter Validation: Base Directory for Hive Proto Hook

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Base Directory for Hive Proto Hook parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_hook_proto_base_directory

Required

true

Suppress Parameter Validation: Hive LLAP Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive LLAP Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_llap_service_env_safety_valve

Required

true

Suppress Parameter Validation: Metastore Transactional Listener List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metastore Transactional Listener List parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_transactional_event_listeners

Required

true

Suppress Configuration Validator: Hive Proxy Groups Validator

Description

Whether to suppress configuration warnings produced by the Hive Proxy Groups Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_groups_validator

Required

true

Suppress Parameter Validation: Hive Metastore Access Control and Proxy User Groups Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Access Control and Proxy User Groups Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_user_groups_list

Required

true

Suppress Configuration Validator: Hive Ranger Validator

Description

Whether to suppress configuration warnings produced by the Hive Ranger Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_validator

Required

true

Suppress Parameter Validation: Replica functions root directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replica functions root directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_repl_replica_functions_root_dir

Required

true

Suppress Parameter Validation: Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_replication_env_safety_valve

Required

true

Suppress Configuration Validator: Hive Sentry Validator

Description

Whether to suppress configuration warnings produced by the Hive Sentry Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_sentry_validator

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_config_safety_valve

Required

true

Suppress Parameter Validation: Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_replication_config_safety_valve

Required

true

Suppress Parameter Validation: LLAP app name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LLAP app name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hivellap_app_name

Required

true

Suppress Parameter Validation: hive.llap.daemon.service.hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the hive.llap.daemon.service.hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hivellap_daemon_service_hosts

Required

true

Suppress Configuration Validator: HiveServer2 Count Validator

Description

Whether to suppress configuration warnings produced by the HiveServer2 Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_count_validator

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_password

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_path

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_basedn

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_domain

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_uri

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_file

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_password

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Hive Lineage Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Lineage Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_lineage_event_log_dir

Required

true

Suppress Configuration Validator: LLAP Proxy Count Validator

Description

Whether to suppress configuration warnings produced by the LLAP Proxy Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_llapproxy_count_validator

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Audit Event Tracker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Tracker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_event_tracker

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_lineage_client_config_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: LLAP Proxy Health

Description

Whether to suppress the results of the LLAP Proxy Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_llap_hive_llap_llapproxy_health

Required

true

Suppress Health Test: HiveServer2 Health

Description

Whether to suppress the results of the HiveServer2 Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_llap_hiveserver2s_healthy

Required

true

Hive on Tez Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hive

API Name

client_config_root_dir

Required

true

Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for hive-site.xml.

Related Name

Default Value

API Name

hive_client_config_safety_valve

Required

false

Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hive-env.sh

Related Name

Default Value

API Name

hive_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

hive_client_java_opts

Required

false

Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server. Consider increasing this if you have tables with a lot of metadata and see timeout errors. Used by most Hive Metastore clients such as Hive CLI and HiveServer2, but not by Impala. Impala has a separately configured timeout.

Related Name

hive.metastore.client.socket.timeout

Default Value

5 minute(s)

API Name

hive_metastore_timeout

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

92

API Name

client_config_priority

Required

true

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

2 GiB

API Name

hive_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

HiveServer2

Advanced

HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hive_hs2_config_safety_valve

Required

false

HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

hive_hs2_env_safety_valve

Required

false

Hive Metastore Connection Retries Count

Description

Number of retries while opening a connection to the Hive Metastore Server

Related Name

hive.metastore.connect.retries

Default Value

10

API Name

hive_metastore_connection_retries

Required

false

Enable Metrics Subsystem

Description

Controls whether the Hive metrics subsystem is enabled for the role.

Related Name

hive.server2.metrics.enabled

Default Value

true

API Name

hive_metrics_enabled

Required

false

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hive/metrics-hivemetastore/metrics.log. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.location

Default Value

API Name

hive_metrics_sample_file_location

Required

false

Metrics Sample File Logging Frequency

Description

The frequency at which the metrics are logged to the sample file. The setting only has an effect if "Enable Metrics Subsystem" is set to true.

Related Name

hive.service.metrics.file.frequency

Default Value

30 second(s)

API Name

hive_metrics_sample_logging_frequency

Required

false

Allow User Substitution

Description

Allow alternate user to be specified as part of HiveServer2 open connection request.

Related Name

hive.server2.allow.user.substitution

Default Value

true

API Name

hive_server2_allow_user_substitution

Required

false

HiveServer2 Transport Mode

Description

The server transport mode.

Related Name

hive.server2.transport.mode

Default Value

binary

API Name

hive_server2_transport_mode

Required

false

Hive Downloaded Resources Directory

Description

Local directory where Hive stores jars downloaded for remote file systems (HDFS). If not specified, Hive uses a default location.

Related Name

hive.downloaded.resources.dir

Default Value

API Name

hiveserver2_downloaded_resources_dir

Required

false

Enable Explain Logging

Description

When enabled, HiveServer2 logs EXPLAIN EXTENDED output for every query at INFO log4j level.

Related Name

hive.log.explain.output

Default Value

false

API Name

hiveserver2_enable_explain_output

Required

false

Hive Local Scratch Directory

Description

Local Directory where Hive stores jars and data when performing a MapJoin optimization. If not specified, Hive uses a default location.

Related Name

hive.exec.local.scratchdir

Default Value

API Name

hiveserver2_exec_local_scratchdir

Required

false

Hive HDFS Scratch Directory

Description

Directory in HDFS where Hive writes intermediate data between MapReduce jobs. If not specified, Hive uses a default location.

Related Name

hive.exec.scratchdir

Default Value

API Name

hiveserver2_exec_scratchdir

Required

false

Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

An XML string that will be inserted verbatim into the Fair Scheduler allocations file. This configuration only has effect in CDH 5.8 or later.

Related Name

Default Value

API Name

hiveserver2_fair_scheduler_safety_valve

Required

false

Idle Operation Timeout

Description

Operation will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero. For a positive value, checked for operations in terminal state only (FINISHED, CANCELED, CLOSED, ERROR). For a negative value, checked for all of the operations regardless of state.

Related Name

hive.server2.idle.operation.timeout

Default Value

6 hour(s)

API Name

hiveserver2_idle_operation_timeout

Required

false

Idle Session Timeout

Description

Session will be closed when not accessed for this duration of time, in milliseconds; disable by setting to zero or a negative value.

Related Name

hive.server2.idle.session.timeout

Default Value

1 day(s)

API Name

hiveserver2_idle_session_timeout

Required

false

Exclude Live Operations From Session Idle Time

Description

Session will be considered to be idle only if there is no activity, and there is no pending operation. This setting takes effect only if session idle timeout (hive.server2.idle.session.timeout) and checking (hive.server2.session.check.interval) are enabled.

Related Name

hive.server2.idle.session.check.operation

Default Value

true

API Name

hiveserver2_idle_session_timeout_check_operation

Required

false

Java Configuration Options for HiveServer2

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hiveserver2_java_opts

Required

false

Maximum Query String Length for Show Locks

Description

The maximum length allowed for the query string when the SHOW LOCKS EXTENDED command is executed. Important: The query string is truncated at the length set for this property. Setting this property to a large value puts pressure on ZooKeeper and might cause out-of-memory issues.

Related Name

hive.lock.query.string.max.length

Default Value

10000

API Name

hiveserver2_lock_query_string_max_length

Required

false

Max HiveServer2 Threads

Description

Maximum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.max.worker.threads

Default Value

500

API Name

hiveserver2_max_threads

Required

true

Min HiveServer2 Threads

Description

Minimum number of worker threads in HiveServer2's thread pool

Related Name

hive.server2.thrift.min.worker.threads

Default Value

5

API Name

hiveserver2_min_threads

Required

true

Session Check Interval

Description

The check interval for session/operation timeout, in milliseconds, which can be disabled by setting to zero or a negative value.

Related Name

hive.server2.session.check.interval

Default Value

15 minute(s)

API Name

hiveserver2_session_check_interval

Required

false

HiveServer2 WebUI Max Threads

Description

The max threads for the HiveServer2 WebUI.

Related Name

hive.server2.webui.max.threads

Default Value

50

API Name

hiveserver2_webui_max_threads

Required

false

HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

hs2_core_site_safety_valve

Required

false

HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HiveServer2 Log Directory

Description

Directory where HiveServer2 will place its log files.

Related Name

Default Value

/var/log/hive

API Name

hive_log_dir

Required

false

Enable Performance Logging

Description

When enabled, it captures time spent during each part of the query execution for the role.

Related Name

hive.server2.performance.logging.enabled

Default Value

true

API Name

hive_performance_logging_enabled

Required

false

Enable HiveServer2 Operations Logging

Description

When enabled, HiveServer2 will temporarily save logs associated with ongoing operations. This enables clients like beeline and Hue to request and display logs for a particular ongoing operation. Logs are removed upon completion of operation.

Related Name

hive.server2.logging.operation.enabled

Default Value

true

API Name

hive_server2_logging_operation_enabled

Required

false

HiveServer2 Operations Log Directory

Description

Top level directory where operation logs are temporarily stored if Enable HiveServer2 Operations Logging is true. Logs are stored in session and operation level subdirectories under this location and are removed on completion of operation.

Related Name

hive.server2.logging.operation.log.location

Default Value

/var/log/hive/operation_logs

API Name

hive_server2_logging_operation_log_location

Required

false

HiveServer2 Logging Threshold

Description

The minimum log level for HiveServer2 logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HiveServer2 Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HiveServer2 Max Log Size

Description

The maximum size, in megabytes, per log file for HiveServer2 logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hive_on_tez_hs2_downloaded_resources_directory_free_space_absolute_thresholds

Required

false

Hive Downloaded Resources Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Downloaded Resources Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Downloaded Resources Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hive_on_tez_hs2_downloaded_resources_directory_free_space_percentage_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

hive_on_tez_hs2_exec_local_scratch_directory_free_space_absolute_thresholds

Required

false

Hive Local Scratch Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Hive Local Scratch Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Hive Local Scratch Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

hive_on_tez_hs2_exec_local_scratch_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hiveserver2_fd_thresholds

Required

false

HiveServer2 Host Health Test

Description

When computing the overall HiveServer2 health, consider the host's health.

Related Name

Default Value

true

API Name

hiveserver2_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

hiveserver2_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

hiveserver2_pause_duration_window

Required

false

HiveServer2 Process Health Test

Description

Enables the health test that the HiveServer2's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hiveserver2_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11121

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'metrics<name=(jvm\.pause.*)><>(.*): (\d+)' name: $1_$2 value: $3

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: strict metric_names: #memory - jvm_buffer_pool_used_bytes - jvm_buffer_pool_capacity_bytes - jvm_buffer_pool_used_buffers - jvm_memory_bytes_used - jvm_memory_bytes_committed - jvm_memory_bytes_max - jvm_memory_bytes_init #gc - jvm_gc_collection_seconds #threads - jvm_threads_current - jvm_threads_daemon - jvm_threads_peak - jvm_threads_started_total - jvm_threads_deadlocked - jvm_threads_deadlocked_monitor - jvm_threads_state #classes - jvm_classes_currently_loaded #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes - jvm_pause_extrasleeptime_count

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Restrict Cross Joins (Cartesian Products)

Description

Whether to allow queries with cross joins. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.cartesian.product

Default Value

false

API Name

hive_restrict_cross_joins

Required

false

Restrict LOAD Queries Against Bucketed Tables

Description

Whether to allow LOAD queries against bucketed tables. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.bucketing

Default Value

true

API Name

hive_restrict_load_bucketed_table

Required

false

Restrict Queries with ORDER BY but no LIMIT clause

Description

Whether to allow queries with an ORDER BY clause, but no LIMIT clause. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.orderby.no.limit

Default Value

false

API Name

hive_restrict_orderby_with_no_limit

Required

false

Restrict Partitioned Table Scans with no Partitioned Column Filter

Description

Whether to allow queries that scan a partitioned table but don't filter on the partition column. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.no.partition.filter

Default Value

false

API Name

hive_restrict_partitioned_scans_no_filter

Required

false

Restrict Unsafe Data Type Comparisons

Description

Whether to allow queries that compare bigints to strings or doubles. If set to true, queries that contain this pattern throw a compile-time error.

Related Name

hive.strict.checks.type.safety

Default Value

true

API Name

hive_restrict_unsafe_comparison

Required

false

HiveServer2 Graceful Shutdown Deadline

Description

Maximum time to wait for ongoing queries to complete before forcing a shutdown of HiveServer2

Related Name

hive.server2.graceful.stop.timeout

Default Value

5 minute(s)

API Name

hive_server2_graceful_stop_timeout

Required

false

HiveServer2 Load Balancer

Description

Address of the load balancer used for HiveServer2 roles, specified in host:port format. If port is not specified, the port used by HiveServer2 is used. Note: Changing this property regenerates Kerberos keytabs for all HiveServer2 roles.

Related Name

Default Value

API Name

hiveserver2_load_balancer

Required

false

Performance

Enable Dynamic Partitions

Description

Whether or not to allow dynamic partitions in DML/DDL.

Related Name

hive.exec.dynamic.partition

Default Value

true

API Name

hive_exec_dynamic_partition

Required

false

Hive Auto Convert Join Noconditional Size

Description

If Hive auto convert join is on, and the sum of the size for n-1 of the tables/partitions for a n-way join is smaller than the specified size, the join is directly converted to a MapJoin (there is no conditional task).

Related Name

hive.auto.convert.join.noconditionaltask.size

Default Value

50 MiB

API Name

hiveserver2_auto_convert_join_noconditionaltask_size

Required

false

Store Intermediate Data on Blobstore

Description

When writing data to a table on a blobstore (such as S3), whether or not the blobstore should be used to store intermediate data during Hive query execution. Setting this to true can degrade performance for queries that spawn multiple MR / Spark jobs, but is useful for queries whose intermediate data cannot fit in the allocated HDFS cluster.

Related Name

hive.blobstore.use.blobstore.as.scratchdir

Default Value

false

API Name

hiveserver2_blobstore_use_blobstore_as_scratchdir

Required

false

Enable Stats Optimization

Description

Enable optimization that checks if a query can be answered using statistics. If so, answers the query using only statistics stored in metastore.

Related Name

hive.compute.query.using.stats

Default Value

true

API Name

hiveserver2_compute_query_using_stats

Required

false

Enable Cost-Based Optimizer for Hive

Description

Enabled the Calcite-based Cost-Based Optimizer for HiveServer2.

Related Name

hive.cbo.enable

Default Value

true

API Name

hiveserver2_enable_cbo

Required

false

Enable MapJoin Optimization

Description

Enable optimization that converts common join into MapJoin based on input file size.

Related Name

hive.auto.convert.join

Default Value

true

API Name

hiveserver2_enable_mapjoin

Required

false

Fetch Task Query Conversion

Description

Some select queries can be converted to a single FETCH task instead of a MapReduce task, minimizing latency. A value of none disables all conversion, minimal converts simple queries such as SELECT * and filter on partition columns, and more converts SELECT queries including FILTERS.

Related Name

hive.fetch.task.conversion

Default Value

more

API Name

hiveserver2_fetch_task_conversion

Required

false

Fetch Task Query Conversion Threshold

Description

Above this size, queries are converted to fetch tasks.

Related Name

hive.fetch.task.conversion.threshold

Default Value

1 GiB

API Name

hiveserver2_fetch_task_conversion_threshold

Required

false

Input Listing Max Threads

Description

Maximum number of threads that Hive uses to list input files. Increasing this value can improve performance when there are a lot of partitions being read, or when running on blobstores.

Related Name

hive.exec.input.listing.max.threads

Default Value

15

API Name

hiveserver2_input_listing_max_threads

Required

false

Maximum ReduceSink Top-K Memory Usage

Description

The maximum percentage of heap to be used for hash in ReduceSink operator for Top-K selection. 0 means the optimization is disabled. Accepted values are between 0 and 1.

Related Name

hive.limit.pushdown.memory.usage

Default Value

0.04

API Name

hiveserver2_limit_pushdown_memory_usage

Required

false

Load Dynamic Partitions Thread Count

Description

Number of threads used to load dynamically generated partitions. Loading requires renaming the file its final location, and updating some metadata about the new partition. Increasing this can improve performance when there are a lot of partitions dynamically generated.

Related Name

hive.load.dynamic.partitions.thread

Default Value

15

API Name

hiveserver2_load_dynamic_partitions_thread_count

Required

false

Enable Map-Side Aggregation

Description

Enable map-side partial aggregation, which cause the mapper to generate fewer rows. This reduces the data to be sorted and distributed to reducers.

Related Name

hive.map.aggr

Default Value

true

API Name

hiveserver2_map_aggr

Required

false

Ratio of Memory Usage for Map-Side Aggregation

Description

Portion of total memory used in map-side partial aggregation. When exceeded, the partially aggregated results will be flushed from the map task to the reducers.

Related Name

hive.map.aggr.hash.percentmemory

Default Value

0.5

API Name

hiveserver2_map_aggr_hash_memory_ratio

Required

false

Enable Merging Small Files - Map-Only Job

Description

Merge small files at the end of a map-only job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapfiles

Default Value

true

API Name

hiveserver2_merge_mapfiles

Required

false

Enable Merging Small Files - Map-Reduce Job

Description

Merge small files at the end of a map-reduce job. When enabled, a map-only job is created to merge the files in the destination table/partitions.

Related Name

hive.merge.mapredfiles

Default Value

false

API Name

hiveserver2_merge_mapredfiles

Required

false

Desired File Size After Merging

Description

The desired file size after merging. This should be larger than hive.merge.smallfiles.avgsize.

Related Name

hive.merge.size.per.task

Default Value

256 MiB

API Name

hiveserver2_merge_size_per_task

Required

false

Small File Average Size Merge Threshold

Description

When the average output file size of a job is less than the value of this property, Hive will start an additional map-only job to merge the output files into bigger files. This is only done for map-only jobs if hive.merge.mapfiles is true, for map-reduce jobs if hive.merge.mapredfiles is true, and for Spark jobs if hive.merge.sparkfiles is true.

Related Name

hive.merge.smallfiles.avgsize

Default Value

16 MiB

API Name

hiveserver2_merge_smallfiles_avgsize

Required

false

MSCK Repair Batch Size

Description

Batch size for the msck repair command (recover partitions command). If the value is greater than zero, new partition information will be sent from HiveServer2 to the Metastore in batches, which can potentially improve memory usage in the Metastore and avoid client read timeout exceptions. If this value is 0, all partition information will sent in a single Thrift call.

Related Name

hive.msck.repair.batch.size

Default Value

3000

API Name

hiveserver2_msck_repair_batch_size

Required

false

Move Files Thread Count

Description

The number of threads used by HiveServer2 to move data from the staging directory to another location (typically to the final table location). A separate thread pool of workers of this size is used for each query, which means this configuration can be set on a per-query basis too.

Related Name

hive.mv.files.thread

Default Value

15

API Name

hiveserver2_mv_files_thread

Required

false

Hive Optimize Sorted Merge Bucket Join

Description

Whether to try sorted merge bucket (SMB) join.

Related Name

hive.optimize.bucketmapjoin.sortedmerge

Default Value

false

API Name

hiveserver2_optimize_bucketmapjoin_sortedmerge

Required

false

Enable Automatic Use of Indexes

Description

Whether to use the indexing optimization for all queries.

Related Name

hive.optimize.index.filter

Default Value

true

API Name

hiveserver2_optimize_index_filter

Required

false

Enable ReduceDeDuplication Optimization

Description

Remove extra map-reduce jobs if the data is already clustered by the same key, eliminating the need to repartition the dataset again.

Related Name

hive.optimize.reducededuplication

Default Value

true

API Name

hiveserver2_optimize_reducededuplication

Required

false

Mininum Reducers for ReduceDeDuplication Optimization

Description

When the number of ReduceSink operators after merging is less than this number, the ReduceDeDuplication optimization will be disabled.

Related Name

hive.optimize.reducededuplication.min.reducer

Default Value

4

API Name

hiveserver2_optimize_reducededuplication_min_reducer

Required

false

Enable Sorted Dynamic Partition Optimizer

Description

When dynamic partition is enabled, reducers keep only one record writer at all times, which lowers the memory pressure on reducers.

Related Name

hive.optimize.sort.dynamic.partition

Default Value

false

API Name

hiveserver2_optimize_sort_dynamic_partition

Required

false

Enable Parallel Compilation of Queries

Description

When activated, individual sessions can compile queries simultaneously. Within each session, queries compile one at a time.

Related Name

hive.driver.parallel.compilation

Default Value

true

API Name

hiveserver2_parallel_compilation_enabled

Required

false

Query Compilation Degree of Parallelism

Description

Determines the maximum number of queries that can compile in parallel on a HiveServer2 instance. Use negative values or zero to set unlimited parallelism. Use a positive value to set the number of queries that can compile simultaneously. This setting can be fine-tuned based on the current cluster load. Monitor cluster load using the 'waiting_compile_ops' metric and the 'Waiting Compile Operations' graph in the HiveServer2 graph library.

Related Name

hive.driver.parallel.compilation.global.limit

Default Value

5

API Name

hiveserver2_parallel_compilation_global_limit

Required

false

Hive SMB Join Cache Rows

Description

The number of rows with the same key value to be cached in memory per SMB-joined table.

Related Name

hive.smbjoin.cache.rows

Default Value

10000

API Name

hiveserver2_smbjoin_cache_rows

Required

false

Load Column Statistics

Description

Whether column stats for a table are fetched during explain.

Related Name

hive.stats.fetch.column.stats

Default Value

true

API Name

hiveserver2_stats_fetch_column_stats

Required

false

Sessions Per Queue

Description

The number of Tez sessions that should be launched on each of the queues specified by "hive.server2.tez.default.queues". Determines the parallelism on each queue.

Related Name

hive.server2.tez.sessions.per.default.queue

Default Value

4

API Name

hiveserver2_tez_sessions_per_default_queue

Required

false

Vectorized Adapter Usage Mode

Description

Vectorized Adaptor Usage Mode specifies the extent to which the vectorization engine tries to vectorize UDFs that do not have native vectorized versions available. Selecting the "none" option specifies that only queries using native vectorized UDFs are vectorized. Selecting the "chosen" option specifies that Hive choses to vectorize a subset of the UDFs based on performance benefits using the Vectorized Adaptor. Selecting the "all" option specifies that the Vectorized Adaptor be used for all UDFs even when native vectorized versions are not available.

Related Name

hive.vectorized.adaptor.usage.mode

Default Value

chosen

API Name

hiveserver2_vectorized_adaptor_usage_mode

Required

false

Enable Vectorization Optimization

Description

Enable optimization that vectorizes query execution by streamlining operations by processing a block of 1024 rows at a time.

Related Name

hive.vectorized.execution.enabled

Default Value

true

API Name

hiveserver2_vectorized_enabled

Required

false

Vectorized GroupBy Check Interval

Description

In vectorized group-by, the number of row entries added to the hash table before re-checking average variable size for memory usage estimation.

Related Name

hive.vectorized.groupby.checkinterval

Default Value

4096

API Name

hiveserver2_vectorized_groupby_checkinterval

Required

false

Vectorized GroupBy Flush Ratio

Description

Ratio between 0.0 and 1.0 of entries in the vectorized group-by aggregation hash that is flushed when the memory threshold is exceeded.

Related Name

hive.vectorized.groupby.flush.percent

Default Value

0.1

API Name

hiveserver2_vectorized_groupby_flush_ratio

Required

false

Enable Vectorized Input Format

Description

If enabled, Hive uses the native vectorized input format for vectorized query execution when it is available.

Related Name

hive.vectorized.use.vectorized.input.format

Default Value

true

API Name

hiveserver2_vectorized_input_format_enabled

Required

false

Exclude Vectorized Input Formats

Description

Specifies a list of file input format classnames to exclude from vectorized query execution using the vectorized input format. Note that vectorized execution can still occur for an excluded input format based on whether row SerDes or vector SerDes are enabled.

Related Name

hive.vectorized.input.format.excludes

Default Value

API Name

hiveserver2_vectorized_input_format_excludes

Required

false

Enable Reduce-Side Vectorization

Description

Whether to vectorize the reduce side of query execution.

Related Name

hive.vectorized.execution.reduce.enabled

Default Value

true

API Name

hiveserver2_vectorized_reduce_enabled

Required

false

Enable Overflow-checked Vector Expressions

Description

To enhance performance, vectorized expressions operate using wide data types like long and double. When wide data types are used, numeric overflows can occur during expression evaluation in a different manner for vectorized expressions than they do for non-vectorized expressions. Consequently, different query results can be returned for vectorized expressions compared to results returned for non-vectorized expressions. When this configuration is enabled, Hive uses vectorized expressions that handle numeric overflows in the same way as non-vectorized expressions are handled.

Related Name

hive.vectorized.use.checked.expressions

Default Value

true

API Name

hiveserver2_vectorized_use_checked_expressions

Required

false

Vectorize Using Vector SerDes

Description

If enabled, Hive uses built-in vector SerDes to process text and sequencefile tables for vectorized query execution.

Related Name

hive.vectorized.use.vector.serde.deserialize

Default Value

false

API Name

hiveserver2_vectorized_use_vector_serde_deserialize

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Thrift port

Description

TCP port number to listen on.

Related Name

hive.server2.thrift.http.port

Default Value

10001

API Name

hive_server2_thrift_http_port

Required

false

Bind HiveServer2 to Wildcard Address

Description

If enabled, the HiveServer2 binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

hive.server2.webui.host

Default Value

true

API Name

hiveserver2_webui_bind_wildcard

Required

false

HiveServer2 WebUI Port

Description

The port the HiveServer2 WebUI will listen on. This can be set to 0 to disable the WebUI.

Related Name

hive.server2.webui.port

Default Value

10002

API Name

hiveserver2_webui_port

Required

false

HiveServer2 Port

Description

Port on which HiveServer2 will listen for connections.

Related Name

hive.server2.thrift.port

Default Value

10000

API Name

hs2_thrift_address_port

Required

false

Resource Management

Java Heap Size of HiveServer2 in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

2 GiB

API Name

hiveserver2_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

HiveServer2 WebUI SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from WebUI SSL.

Related Name

hive.server2.webui.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_webui_exclude_ciphersuites

Required

false

Enable TLS/SSL for HiveServer2 WebUI

Description

Encrypt communication between clients and HiveServer2 WebUI using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.webui.use.ssl

Default Value

false

API Name

ssl_enabled

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 WebUI is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.webui.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 WebUI keystore file.

Related Name

hive.server2.webui.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_config_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Parameter Validation: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Operations Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Parameter Validation: Thrift port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Thrift port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_thrift_http_port

Required

true

Suppress Parameter Validation: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Downloaded Resources Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Parameter Validation: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Local Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Parameter Validation: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive HDFS Scratch Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Parameter Validation: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for HiveServer2 parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Parameter Validation: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Parameter Validation: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Vectorized Input Formats parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Parameter Validation: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Parameter Validation: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Parameter Validation: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: HiveServer2 Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 WebUI TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_pause_duration

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hiveserver2_unexpected_exits

Required

true

Suppress Health Test: Hive Downloaded Resources Directory Free Space

Description

Whether to suppress the results of the Hive Downloaded Resources Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hs2_downloaded_resources_directory_free_space

Required

true

Suppress Health Test: Hive Local Scratch Directory Free Space

Description

Whether to suppress the results of the Hive Local Scratch Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive_on_tez_hs2_exec_local_scratch_directory_free_space

Required

true

Service-Wide

Advanced

Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

For advanced use only, a string to be inserted into atlas-application.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

application_properties_safety_valve

Required

false

Hive Auxiliary JARs Directory

Description

Directory containing auxiliary JARs used by Hive. This should be a directory location and not a classpath containing one or more JARs. This directory must be created and managed manually on hosts that run the Hive Metastore Server, HiveServer2, or the Hive CLI. The directory location is set in the environment as HIVE_AUX_JARS_PATH and will generally override the hive.aux.jars.path property set in XML files, even if hive.aux.jars.path is set in an advanced configuration snippet.

Related Name

Default Value

API Name

hive_aux_jars_path_dir

Required

false

Bypass Hive Metastore Server

Description

Instead of talking to Hive Metastore Server for Metastore information, Hive clients will talk directly to the Metastore database.

Related Name

Default Value

false

API Name

hive_bypass_metastore_server

Required

false

Aborted Transaction Threshold

Description

Number of aborted transactions involving a particular table or partition before major compaction is initiated.

Related Name

hive.compactor.abortedtxn.threshold

Default Value

1000

API Name

hive_compactor_abortedtxn_threshold

Required

true

Number of Threads Used by Compactor

Description

Number of compactor worker threads to run on this metastore instance. Can be different values on different Metastore instances.

Related Name

hive.compactor.worker.threads

Default Value

5

API Name

hive_compactor_worker_threads

Required

true

Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_core_site_safety_valve

Required

false

Default Table Format - Create Tables as Full ACID

Description

Whether the eligible tables should be created as full ACID by default. Does not apply to external tables, the ones using storage handlers, etc.

Related Name

hive.create.as.acid

Default Value

true

API Name

hive_create_as_acid

Required

false

Default Table Format - Create Tables as ACID Insert Only

Description

Whether the eligible tables should be created as ACID insert-only by default. Does not apply to external tables, the ones using storage handlers, etc.

Related Name

hive.create.as.insert.only

Default Value

true

API Name

hive_create_as_insert_only

Required

false

Hive Copy Large File Size

Description

Smaller than this size, Hive uses a single-threaded copy; larger than this size, Hive uses DistCp.

Related Name

hive.exec.copyfile.maxsize

Default Value

32 MiB

API Name

hive_exec_copyfile_maxsize

Required

false

Base Directory for Hive Proto Hook

Description

The directory where hive proto hooks should write the events, should generally be location of query_data table under sys.db database.

Related Name

hive.hook.proto.base-directory

Default Value

/warehouse/tablespace/managed/hive/sys.db/query_data/

API Name

hive_hook_proto_base_directory

Required

false

Run compactor on Hive Metastore or HiveServer2.

Description

Choose where the compactor worker threads should run. Only possible values are metastore or hs2.

Related Name

hive.metastore.runworker.in

Default Value

hs2

API Name

hive_metastore_runworker_in

Required

true

Metastore Transactional Listener List

Description

A comma separated list of Java classes that implement the org.apache.hadoop.hive.metastore.MetaStoreEventListener interface. Both the metastore event and corresponding listener method will be invoked in the same JDO transaction.

Related Name

hive.metastore.transactional.event.listeners

Default Value

org.apache.hive.hcatalog.listener.DbNotificationListener

API Name

hive_metastore_transactional_event_listeners

Required

false

Hive on Tez Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

HIVE_ON_TEZ_service_env_safety_valve

Required

false

Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the environment of Hive replication jobs.

Related Name

Default Value

API Name

hive_replication_env_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hive_service_config_safety_valve

Required

false

Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only, a string to be inserted into hive-site.xml. Applies to all Hive Replication jobs.

Related Name

Default Value

API Name

hive_service_replication_config_safety_valve

Required

false

Use Locking

Description

Support concurrency and use locks, needed for Transactions. Requires Zookeeper.

Related Name

hive.support.concurrency

Default Value

true

API Name

hive_support_concurrency

Required

false

Transaction Manager

Description

HiveTxnManager implementation used for managing transactions.

Related Name

hive.txn.manager

Default Value

org.apache.hadoop.hive.ql.lockmgr.DbTxnManager

API Name

hive_txn_manager

Required

true

Transaction Maximum Open Batch

Description

Maximum number of transactions that can be fetched in one call to open_txns(). Increasing this will decrease the number of delta files created when streaming data into Hive. But it will also increase the number of open transactions at any given time, possibly impacting read performance.

Related Name

hive.txn.max.open.batch

Default Value

1000

API Name

hive_txn_max_open_batch

Required

true

Transaction Strict Locking Mode

Description

In strict locking non-ACID resources use standard R/W lock semantics.

Related Name

hive.txn.strict.locking.mode

Default Value

false

API Name

hive_txn_strict_locking_mode

Required

false

Transaction Timeout

Description

Time after which transactions are declared aborted if the client has not sent a heartbeat.

Related Name

hive.txn.timeout

Default Value

5 minute(s)

API Name

hive_txn_timeout

Required

true

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hive

API Name

process_username

Required

true

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

For advanced use only, a string to be inserted into ranger-hive-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-hive-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

For advanced use only, a string to be inserted into ranger-hive-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/hive/audit

API Name

audit_event_log_dir

Required

false

Hive Lineage Log Directory

Description

The directory in which Hive lineage log files are written.

Related Name

lineage_event_log_dir

Default Value

/var/log/hive/lineage

API Name

lineage_event_log_dir

Required

true

Hive Maximum Lineage Log File Size

Description

The maximum size, in megabytes, per log file for Hive lineage logs. Typically used by log4j or logback.

Related Name

max_lineage_log_file_size

Default Value

100 MiB

API Name

max_lineage_log_file_size

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Number of Audit Logs to Retain

Description

Maximum number of rolled-over audit logs to retain. The logs are not deleted if they contain audit events that have not yet been propagated to the Audit Server.

Related Name

navigator.client.max_num_audit_log

Default Value

10

API Name

navigator_client_max_num_audit_log

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Hive Compaction Health Test

Description

Enables the health test that checks whether compaction processes are properly configured and operational.

Related Name

Default Value

false

API Name

hive_compaction_health_check_enabled

Required

false

Healthy HiveServer2 Monitoring Thresholds

Description

The health test thresholds of the overall HiveServer2 health. The check returns "Concerning" health if the percentage of "Healthy" HiveServer2s falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" HiveServer2s falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hive_on_tez_hiveserver2s_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>hive.metastore.client.socket.timeout</name> <value>60</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Atlas Service

Description

Name of the Atlas service that this Hive service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Generate HADOOP_CREDSTORE_PASSWORD

Description

Flag to enable or disable the generation of HADOOP_CREDSTORE_PASSWORD.

Related Name

generate_jceks_password

Default Value

true

API Name

generate_jceks_password

Required

false

HBase Service

Description

Name of the HBase service that this Hive service instance depends on.

Related Name

Default Value

API Name

hbase_service

Required

false

HDFS Service

Description

Name of the HDFS service that this Hive service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Enable Asynchronous Logging

Description

Asynchronous Log4j2 logging can give a significant performance improvement as logging will be handled in a separate thread that uses an LMAX disruptor queue for buffering log messages. Refer to https://logging.apache.org/log4j/2.x/manual/async.html for benefits and drawbacks. For debugging issues we recommend setting this to false.

Related Name

hive.async.log.enabled

Default Value

false

API Name

hive_async_log_enabled

Required

false

Hive Bytes Per Reducer

Description

Size per reducer. If the input size is 10GiB and this is set to 1GiB, Hive will use 10 reducers.

Related Name

hive.exec.reducers.bytes.per.reducer

Default Value

64 MiB

API Name

hive_bytes_per_reducer

Required

false

Default File Format

Description

Default file format for CREATE TABLE statement.

Related Name

hive.default.fileformat

Default Value

TextFile

API Name

hive_default_fileformat

Required

true

Default File Format for Managed Tables

Description

Default file format for CREATE TABLE statement applied to managed tables only. External tables will be created with default file format. Leaving this null will result in using the default file format for all tables.

Related Name

hive.default.fileformat.managed

Default Value

ORC

API Name

hive_default_fileformat_managed

Required

false

Hive Max Reducers

Description

Max number of reducers to use. If the configuration parameter Hive Reduce Tasks is negative, Hive will limit the number of reducers to the value of this parameter.

Related Name

hive.exec.reducers.max

Default Value

1009

API Name

hive_max_reducers

Required

false

Hive Reduce Tasks

Description

Default number of reduce tasks per job. Usually set to a prime number close to the number of available hosts. Ignored when mapred.job.tracker is "local". Hadoop sets this to 1 by default, while Hive uses -1 as the default. When set to -1, Hive will automatically determine an appropriate number of reducers for each job.

Related Name

mapred.reduce.tasks

Default Value

-1

API Name

hive_reduce_tasks

Required

false

Support Dynamic Service Discovery

Description

Whether HiveServer2 supports dynamic service discovery for its clients. To support this, each instance of HiveServer2 currently uses ZooKeeper to register itself, when it is brought up. JDBC/ODBC clients should use the ZooKeeper ensemble: hive.zookeeper.quorum in their connection string.

Related Name

hive.server2.support.dynamic.service.discovery

Default Value

true

API Name

hive_server2_support_dynamic_service_discovery

Required

false

Hive Server Zookeeper Namespace

Description

The parent node in ZooKeeper used by HiveServer2 when supporting dynamic service discovery.

Related Name

hive.server2.zookeeper.namespace

Default Value

hiveserver2

API Name

hive_server2_zookeeper_namespace

Required

false

Set User and Group Information

Description

In unsecure mode, setting this property to true will cause the Metastore Server to execute DFS operations using the client's reported user and group permissions. Cloudera Manager will set this for all clients and servers.

Related Name

hive.metastore.execute.setugi

Default Value

true

API Name

hive_set_ugi

Required

true

Table migration control file URL

Description

Applicable for upgrade. If set, migration tool will expect either a YAML file on this URL, or a directory with YAML files in it. Such YAML file(s) shall contain which tables in which databases should the tool care about. The value here will be parsed and handled by Hadoop filesystem, therefore absolute paths with schemes are required (e.g hdfs:/path or file:/path). HDFS paths are recommended so that locality wouldn't cause any surprises.

Related Name

Default Value

API Name

hive_table_migration_control_file_url

Required

false

HiveServer2 Enable Impersonation

Description

HiveServer2 will impersonate the beeline client user when talking to other services such as MapReduce and HDFS.

Related Name

hive.server2.enable.doAs

Default Value

false

API Name

hiveserver2_enable_impersonation

Required

false

LDAP password

Description

LDAP password for Hive 3 replication

Related Name

Default Value

API Name

hiveserver2_ldap_replication_password

Required

false

LDAP username

Description

LDAP username for Hive 3 replication

Related Name

Default Value

API Name

hiveserver2_ldap_replication_user

Required

false

Hive Metastore Connector

Description

Name of the Hive Metastore Connector from the data context that this service instance depends on.

Related Name

Default Value

API Name

hms_connector

Required

true

MapReduce Service

Description

MapReduce jobs are run against this service.

Related Name

Default Value

API Name

mapreduce_yarn_service

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hive.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin URL Auth Filesystem Schemes

Description

Set Ranger URL Auth Filesystem Schemes.

Related Name

ranger.plugin.hive.urlauth.filesystem.schemes

Default Value

hdfs:, file:, wasb:, adl:

API Name

ranger_plugin_urlauth_filesystem_schemes

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hive.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Hive service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Enable Dynamic Numbers of Reducers

Description

Turn on Tez' auto reducer parallelism feature. When enabled, Hive will still estimate data sizes and set parallelism estimates. Tez will sample source vertices' output sizes and adjust the estimates at runtime as necessary.

Related Name

hive.tez.auto.reducer.parallelism

Default Value

true

API Name

tez_auto_reducer_parallelism

Required

false

Tez Bucket Pruning

Description

When pruning is enabled, filters on bucket columns will be processed by filtering the splits against a bitset of included buckets. This needs predicates produced by hive.optimize.ppd and hive.optimize.index.filters.

Related Name

hive.tez.bucket.pruning

Default Value

true

API Name

tez_bucket_pruning

Required

false

Tez Cartesian-product Enabled

Description

Use Tez cartesian product edge for Hive cartesian product

Related Name

hive.tez.cartesian-product.enabled

Default Value

true

API Name

tez_cartesian_product_enabled

Required

false

Tez Container Size

Description

By default, Tez uses the java options from map tasks. Use this property to override that value.

Related Name

hive.tez.container.size

Default Value

4096

API Name

tez_container_size

Required

false

Tez CPU vCores

Description

By default Tez will ask for however many cpus map-reduce is configured to use per container. This can be used to overwrite.

Related Name

hive.tez.cpu.vcores

Default Value

-1

API Name

tez_cpu_vcores

Required

false

Tez Dynamic Partition Pruning Max Event Size

Description

Maximum size of events sent by processors in dynamic pruning. If this size is crossed no pruning will take place.

Related Name

hive.tez.dynamic.partition.pruning.max.event.size

Default Value

1048576

API Name

tez_dynamic_partition_max_event_size

Required

false

Enable Dynamic Partition Pruning

Description

When dynamic pruning is enabled, joins on partition keys will be processed by sending events from the processing vertices to the tez application master. These events will be used to prune unnecessary partitions.

Related Name

hive.tez.dynamic.partition.pruning

Default Value

true

API Name

tez_dynamic_partition_pruning

Required

false

Tez Dynamic Partition Pruning Max Data Size

Description

Maximum total data size of events in dynamic pruning.

Related Name

hive.tez.dynamic.partition.pruning.max.data.size

Default Value

104857600

API Name

tez_dynamic_partition_pruning_max_data_size

Required

false

Tez Exec Print Summary

Description

Display breakdown of execution steps, for every query executed by the shell.

Related Name

hive.tez.exec.print.summary

Default Value

true

API Name

tez_exec_print_summary

Required

false

Tez Input Format

Description

The default input format for Tez. Tez groups splits in the Application Master.

Related Name

hive.tez.input.format

Default Value

org.apache.hadoop.hive.ql.io.HiveInputFormat

API Name

tez_input_format

Required

false

Tez Input Generate Consistent Splits

Description

Whether to generate consistent split locations when generating splits in the AM

Related Name

hive.tez.input.generate.consistent.splits

Default Value

true

API Name

tez_input_generate_consistent_splits

Required

false

Tez Java Options

Description

Java command line options for Tez.

Related Name

hive.tez.java.opts

Default Value

-server -Djava.net.preferIPv4Stack=true -XX:NewRatio=8 -XX:+UseNUMA -XX:+UseG1GC -XX:+ResizeTLAB -XX:+PrintGCDetails -verbose:gc

API Name

tez_java_opts

Required

false

Tez Log Level

Description

The log level to use for tasks executing as part of the DAG. Used only if hive.tez.java.opts is used to configure Java options.

Related Name

hive.tez.log.level

Default Value

INFO

API Name

tez_log_level

Required

false

Tez Max Partition Factor

Description

When auto reducer parallelism is enabled this factor will be used to over-partition data in shuffle edges.

Related Name

hive.tez.max.partition.factor

Default Value

2.0

API Name

tez_max_partition_factor

Required

false

Tez Min Partition Factor

Description

When auto reducer parallelism is enabled this factor will be used to put a lower limit to the number of reducers that tez specifies.

Related Name

hive.tez.min.partition.factor

Default Value

0.25

API Name

tez_min_partition_factor

Required

false

Tez Service

Description

Tez Service that the Hive on Tez uses for execution

Related Name

Default Value

API Name

tez_service

Required

true

Tez SMB Number of Waves

Description

The number of waves in which to run the SMB join. Account for cluster being occupied. Ideally should be 1 wave.

Related Name

hive.tez.smb.number.waves

Default Value

0.5

API Name

tez_smb_number_waves

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Hive service instance depends on.

Related Name

Default Value

API Name

zookeeper_service

Required

false

Proxy

Hive Metastore Access Control and Proxy User Groups Override

Description

This configuration overrides the value set for Hive Proxy User Groups configuration in HDFS service for use by Hive Metastore Server. Specify a comma-delimited list of groups that you want to allow access to Hive Metastore metadata and allow the Hive user to impersonate. A value of '*' allows all groups. The default value of empty inherits the value set for Hive Proxy User Groups configuration in the HDFS service.

Related Name

hadoop.proxyuser.hive.groups

Default Value

API Name

hive_proxy_user_groups_list

Required

false

Replication

Replica functions root directory

Description

Root directory on the replica warehouse where the repl sub-system will store jars from the primary warehouse

Related Name

hive.repl.replica.functions.root.dir

Default Value

API Name

hive_repl_replica_functions_root_dir

Required

false

Security

Atlas Kafka Messages Spool Directory

Description

Spool directory for Atlas Kafka Messages.

Related Name

atlas.hook.spool.dir

Default Value

/var/log/hive/atlas-spool

API Name

atlas_message_spool_path

Required

false

Enable LDAP Authentication for HiveServer2

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

Default Value

false

API Name

hiveserver2_enable_ldap_auth

Required

false

Enable TLS/SSL for HiveServer2

Description

Encrypt communication between clients and HiveServer2 using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hive.server2.use.SSL

Default Value

false

API Name

hiveserver2_enable_ssl

Required

false

HiveServer2 SSL Exclude Cipher Suites

Description

The cipher suites should be excluded from Hiveserver2 SSL.

Related Name

hive.server2.http.exclude.ciphersuites

Default Value

modern2018

API Name

hiveserver2_exclude_ciphersuites

Required

false

HiveServer2 SSL Include Cipher Suites

Description

The cipher suites should be included in Hiverserver2 SSL.

Related Name

hive.server2.binary.include.ciphersuites

Default Value

modern2018

API Name

hiveserver2_include_ciphersuites

Required

false

HiveServer2 TLS/SSL Server Keystore File Password

Description

The password for the HiveServer2 keystore file.

Related Name

hive.server2.keystore.password

Default Value

API Name

hiveserver2_keystore_password

Required

false

HiveServer2 TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HiveServer2 is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

hive.server2.keystore.path

Default Value

API Name

hiveserver2_keystore_path

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like "uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

hive.server2.authentication.ldap.baseDN

Default Value

API Name

hiveserver2_ldap_basedn

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

hive.server2.authentication.ldap.Domain

Default Value

API Name

hiveserver2_ldap_domain

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

hive.server2.authentication.ldap.url

Default Value

API Name

hiveserver2_ldap_uri

Required

false

HiveServer2 TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HiveServer2 might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

hiveserver2_truststore_file

Required

false

HiveServer2 TLS/SSL Trust Store Password

Description

The password for the HiveServer2 TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

hiveserver2_truststore_password

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hive

API Name

kerberos_princ_name

Required

true

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/hive

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/hive/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hive/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hive.policy.cache.dir

Default Value

/var/lib/ranger/hive/policy-cache

API Name

ranger_policy_cache_dir

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hive Client Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hive-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_client_java_opts

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_config_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HiveServer2 Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_hs2_env_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Log Directory

Description

Whether to suppress configuration warnings produced by the HiveServer2 Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_log_dir

Required

true

Suppress Configuration Validator: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the Metrics Sample File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Restrict Load Bucketed Table Validator

Description

Whether to suppress configuration warnings produced by the Restrict Load Bucketed Table Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_load_bucketed_table_validator

Required

true

Suppress Configuration Validator: Restrict Unsafe Comparison Validator

Description

Whether to suppress configuration warnings produced by the Restrict Unsafe Comparison Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_restrict_unsafe_comparison_validator

Required

true

Suppress Configuration Validator: HiveServer2 Operations Log Directory

Description

Whether to suppress configuration warnings produced by the HiveServer2 Operations Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_logging_operation_log_location

Required

true

Suppress Configuration Validator: Thrift port

Description

Whether to suppress configuration warnings produced by the Thrift port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hive_server2_thrift_http_port

Required

true

Suppress Configuration Validator: Hive Downloaded Resources Directory

Description

Whether to suppress configuration warnings produced by the Hive Downloaded Resources Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_downloaded_resources_dir

Required

true

Suppress Configuration Validator: Hive Local Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive Local Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_local_scratchdir

Required

true

Suppress Configuration Validator: Hive HDFS Scratch Directory

Description

Whether to suppress configuration warnings produced by the Hive HDFS Scratch Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_exec_scratchdir

Required

true

Suppress Configuration Validator: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_fair_scheduler_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for HiveServer2

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for HiveServer2 configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_java_opts

Required

true

Suppress Configuration Validator: HiveServer2 Load Balancer

Description

Whether to suppress configuration warnings produced by the HiveServer2 Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_load_balancer

Required

true

Suppress Configuration Validator: Exclude Vectorized Input Formats

Description

Whether to suppress configuration warnings produced by the Exclude Vectorized Input Formats configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_vectorized_input_format_excludes

Required

true

Suppress Configuration Validator: HiveServer2 WebUI Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hiveserver2_webui_port

Required

true

Suppress Configuration Validator: HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the HiveServer2 Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_core_site_safety_valve

Required

true

Suppress Configuration Validator: HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the HiveServer2 Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_thrift_address_port

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: HiveServer2 WebUI TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the HiveServer2 WebUI TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_application_properties_safety_valve

Required

true

Suppress Parameter Validation: Atlas Kafka Messages Spool Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Kafka Messages Spool Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_message_spool_path

Required

true

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Hive Auxiliary JARs Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Auxiliary JARs Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_aux_jars_path_dir

Required

true

Suppress Configuration Validator: Client TLS/SSL In Use With LDAP Authentication Validator

Description

Whether to suppress configuration warnings produced by the Client TLS/SSL In Use With LDAP Authentication Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_client_ssl_recommended_with_ldap_auth_validator

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_core_site_safety_valve

Required

true

Suppress Parameter Validation: Default File Format for Managed Tables

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default File Format for Managed Tables parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_default_fileformat_managed

Required

true

Suppress Parameter Validation: Base Directory for Hive Proto Hook

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Base Directory for Hive Proto Hook parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_hook_proto_base_directory

Required

true

Suppress Parameter Validation: Metastore Transactional Listener List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metastore Transactional Listener List parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_metastore_transactional_event_listeners

Required

true

Suppress Parameter Validation: Hive on Tez Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive on Tez Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_on_tez_service_env_safety_valve

Required

true

Suppress Configuration Validator: Hive Proxy Groups Validator

Description

Whether to suppress configuration warnings produced by the Hive Proxy Groups Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_groups_validator

Required

true

Suppress Parameter Validation: Hive Metastore Access Control and Proxy User Groups Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Metastore Access Control and Proxy User Groups Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_proxy_user_groups_list

Required

true

Suppress Configuration Validator: Ranger Plugin Url Auth Validator for filesystem schemes

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Url Auth Validator for filesystem schemes configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_url_auth_validator

Required

true

Suppress Configuration Validator: Hive Ranger Validator

Description

Whether to suppress configuration warnings produced by the Hive Ranger Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_validator

Required

true

Suppress Parameter Validation: Replica functions root directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replica functions root directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_repl_replica_functions_root_dir

Required

true

Suppress Parameter Validation: Hive Replication Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_replication_env_safety_valve

Required

true

Suppress Configuration Validator: Hive Sentry Validator

Description

Whether to suppress configuration warnings produced by the Hive Sentry Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_sentry_validator

Required

true

Suppress Parameter Validation: Hive Server Zookeeper Namespace

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Server Zookeeper Namespace parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_server2_zookeeper_namespace

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_config_safety_valve

Required

true

Suppress Parameter Validation: Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Replication Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_service_replication_config_safety_valve

Required

true

Suppress Parameter Validation: Table migration control file URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Table migration control file URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hive_table_migration_control_file_url

Required

true

Suppress Configuration Validator: HiveServer2 Count Validator

Description

Whether to suppress configuration warnings produced by the HiveServer2 Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_count_validator

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_password

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_keystore_path

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_basedn

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_domain

Required

true

Suppress Parameter Validation: LDAP password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_replication_password

Required

true

Suppress Parameter Validation: LDAP username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP username parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_replication_user

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_ldap_uri

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_file

Required

true

Suppress Parameter Validation: HiveServer2 TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HiveServer2 TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hiveserver2_truststore_password

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Hive Lineage Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Lineage Log Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_lineage_event_log_dir

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Plugin URL Auth Filesystem Schemes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin URL Auth Filesystem Schemes parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_urlauth_filesystem_schemes

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Tez Input Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Input Format parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez_input_format

Required

true

Suppress Parameter Validation: Tez Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Java Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez_java_opts

Required

true

Suppress Parameter Validation: Tez Log Level

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Log Level parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez_log_level

Required

true

Suppress Health Test: Compaction System Health Check

Description

Whether to suppress the results of the Compaction System Health Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_on_tez_compaction_health

Required

true

Suppress Health Test: HiveServer2 Health

Description

Whether to suppress the results of the HiveServer2 Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hive_on_tez_hiveserver2s_healthy

Required

true

Hue Properties in Cloudera Runtime 7.2.18

Role groups:

Hue Server

Advanced

Top Banner Custom HTML

Description

An optional, custom one-line HTML code to display as a banner on top of all Hue Server web pages. Useful in displaying cluster identity of the Hue Server.

Related Name

banner_top_html

Default Value

API Name

banner_html

Required

false

Hue Server Advanced Configuration Snippet (Safety Valve) for impalad_flags

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to impalad_flags for this role only. Key names should begin with a hyphen(-). For example: -log_filename=foo.log

Related Name

Default Value

API Name

hue_impalad_flags_safety_valve

Required

false

Metrics Sample File Location

Description

The full path to a file with a sample of metrics exposed by the role. The sample is updated at the frequency configured by Metrics Sample File Logging Frequency. By default, the sample file is logged to a directory under the role log directory, e.g., /var/log/hue/metrics-hue_server/metrics.log.

Related Name

location

Default Value

API Name

hue_metrics_sample_file_location

Required

false

Metrics Sample File Logging Frequency

Description

The frequency at which the metrics are logged to the sample file.

Related Name

collection_interval

Default Value

30 second(s)

API Name

hue_metrics_sample_logging_frequency

Required

false

Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

For advanced use only. A string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

hue_server_hive_safety_valve

Required

false

Hue Server Advanced Configuration Snippet (Safety Valve) for hue_safety_valve_server.ini

Description

For advanced use only. A string to be inserted into hue_safety_valve_server.ini for this role only.

Related Name

Default Value

API Name

hue_server_hue_safety_valve

Required

false

Hue Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HUE_SERVER_role_env_safety_valve

Required

false

Hue Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to sqoop.properties for this role only. Used in the Sqoop App for connecting to the Sqoop Service.

Related Name

Default Value

API Name

hue_sqoop2_properties_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

40

API Name

process_start_secs

Required

false

Logs

Hue Server Log Directory

Description

Directory where Hue Server will place its log files.

Related Name

Default Value

/var/log/hue

API Name

hue_server_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hue_server_fd_thresholds

Required

false

Hue Server Host Health Test

Description

When computing the overall Hue Server health, consider the host's health.

Related Name

Default Value

true

API Name

hue_server_host_health_enabled

Required

false

Hue Server Process Health Test

Description

Enables the health test that the Hue Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hue_server_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

hue_server_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

hue_server_web_metric_collection_thresholds

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings

using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HiveServer2 and Impala Thrift Connection Timeout

Description

Timeout in seconds for Thrift calls to HiveServer2 and Impala.

Related Name

server_conn_timeout

Default Value

2 minute(s)

API Name

hs2_conn_timeout

Required

false

Jobsub Examples and Templates Directory

Description

Location on HDFS where the jobsub examples and templates are stored.

Related Name

remote_data_dir

Default Value

/user/hue/jobsub

API Name

hue_server_remote_data_dir

Required

true

Secret Key

Description

Random string used for secure hashing in the session store.

Related Name

secret_key

Default Value

API Name

secret_key

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Hue HTTP Port

Description

Port to use to connect to the Hue server.

Related Name

http_port

Default Value

8888

API Name

hue_http_port

Required

false

Bind Hue Server to Wildcard Address

Description

If enabled, the Hue server binds to the wildcard address ("0.0.0.0") for its ports.

Related Name

Default Value

false

API Name

hue_server_bind_wildcard

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable Log and Query Redaction (Hue Only)

Description

Enable/Disable the Log and Query Redaction Policy for Hue. If enabled, and "Enable Log and Query Redaction" in HDFS is also enabled, Hue logs will be redacted using the defined Log and Query Redaction Policy. If disabled, log redaction will not take place even if "Enable Log and Query Redaction" is enabled in HDFS. Uncheck this property if Hue is unresponsive when custom redaction rules are in place.

Related Name

redaction_policy_enabled

Default Value

true

API Name

hue_server_redaction_policy_enabled

Required

false

Hue TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Hue is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

ssl_cacerts

Default Value

API Name

ssl_cacerts

Required

false

Hue TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Hue is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_certificate

Default Value

API Name

ssl_certificate

Required

false

Enable TLS/SSL for Hue

Description

Encrypt communication between clients and Hue using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

Default Value

false

API Name

ssl_enable

Required

false

Hue TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Hue is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_private_key

Default Value

API Name

ssl_private_key

Required

false

Hue TLS/SSL Private Key Password

Description

The password for the private key in the Hue TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

ssl_password

Default Value

API Name

ssl_private_key_password

Required

false

Suppressions

Suppress Parameter Validation: Top Banner Custom HTML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Top Banner Custom HTML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_banner_html

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hue HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_http_port

Required

true

Suppress Parameter Validation: Hue Server Advanced Configuration Snippet (Safety Valve) for impalad_flags

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Advanced Configuration Snippet (Safety Valve) for impalad_flags parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_impalad_flags_safety_valve

Required

true

Suppress Parameter Validation: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Sample File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_metrics_sample_file_location

Required

true

Suppress Parameter Validation: Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_hive_safety_valve

Required

true

Suppress Parameter Validation: Hue Server Advanced Configuration Snippet (Safety Valve) for hue_safety_valve_server.ini

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Advanced Configuration Snippet (Safety Valve) for hue_safety_valve_server.ini parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_hue_safety_valve

Required

true

Suppress Parameter Validation: Hue Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_log_dir

Required

true

Suppress Parameter Validation: Jobsub Examples and Templates Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Jobsub Examples and Templates Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_remote_data_dir

Required

true

Suppress Parameter Validation: Hue Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Hue Server Safety Valve Format Validator

Description

Whether to suppress configuration warnings produced by the Hue Server Safety Valve Format Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_safety_valve_format_validator

Required

true

Suppress Parameter Validation: Hue Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_sqoop2_properties_safety_valve

Required

true

Suppress Configuration Validator: Hue TLS/SSL Validator

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_ssl_validator

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Secret Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secret Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secret_key

Required

true

Suppress Parameter Validation: Hue TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_cacerts

Required

true

Suppress Parameter Validation: Hue TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_certificate

Required

true

Suppress Parameter Validation: Hue TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_private_key

Required

true

Suppress Parameter Validation: Hue TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_private_key_password

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_server_web_metric_collection

Required

true

Kerberos Ticket Renewer

Advanced

Kerberos Ticket Renewer Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KT_RENEWER_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Kerberos Ticket Renewer Log Directory

Description

Directory where Kerberos Ticket Renewer will place its log files.

Related Name

Default Value

/var/log/hue

API Name

kt_renewer_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kt_renewer_fd_thresholds

Required

false

Kerberos Ticket Renewer Host Health Test

Description

When computing the overall Kerberos Ticket Renewer health, consider the host's health.

Related Name

Default Value

true

API Name

kt_renewer_host_health_enabled

Required

false

Kerberos Ticket Renewer Process Health Test

Description

Enables the health test that the Kerberos Ticket Renewer's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kt_renewer_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Hue Keytab Renewal Interval

Description

Interval in seconds with which Hue's Kerberos ticket will get renewed.

Related Name

reinit_frequency

Default Value

1 hour(s)

API Name

keytab_reinit_frequency

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Kerberos Ticket Renewer Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Ticket Renewer Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kt_renewer_log_dir

Required

true

Suppress Parameter Validation: Kerberos Ticket Renewer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Ticket Renewer Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kt_renewer_role_env_safety_valve

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kt_renewer_unexpected_exits

Required

true

Load Balancer

Advanced

Load Balancer Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HUE_LOAD_BALANCER_role_env_safety_valve

Required

false

Load Balancer Advanced Configuration Snippet (Safety Valve) for httpd.conf

Description

For advanced use only, a string to be inserted into httpd.conf for this role only. This can only add options to the configuration, and cannot override previously defined options.

Related Name

Default Value

API Name

hue_load_balancer_safety_valve

Required

false

Hue Load Balancer Cookie Refresh

Description

Force refresh the Apache BalancerMember cookie value to rebalance Hue backend connections.

Related Name

huelb_cookie_refresh

Default Value

false

API Name

huelb_cookie_refresh

Required

true

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

SSLCipherSuite

Description

This directive uses a colon-separated cipher-spec string consisting of OpenSSL cipher specifications to configure the Cipher Suite the client is permitted to negotiate in the SSL handshake phase.

Related Name

SSLCipherSuite

Default Value

ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384 !DSS

API Name

ssl_cipher_suite

Required

false

SSLProtocol

Description

This directive can be used to control which versions of the SSL/TLS protocol will be accepted in new connections by Hue Load Balancer.

Related Name

SSLProtocol

Default Value

+TLSv1.2

API Name

ssl_protocol

Required

false

Logs

Hue Load Balancer Log Directory

Description

Directory where Hue Load Balancer will place its log files.

Related Name

Default Value

/var/log/hue-httpd

API Name

hue_load_balancer_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hue_load_balancer_fd_thresholds

Required

false

Load Balancer Host Health Test

Description

When computing the overall Load Balancer health, consider the host's health.

Related Name

Default Value

true

API Name

hue_load_balancer_host_health_enabled

Required

false

Load Balancer Process Health Test

Description

Enables the health test that the Load Balancer's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hue_load_balancer_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Hue Load Balancer Port

Description

Port to use to connect to the Hue through the Load Balancer.

Related Name

Listen

Default Value

8889

API Name

listen

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog

Description

The path to the file containing the passphrase used to encrypt the private key of the Hue Load Balancer server. The passphrase file is optional.

Related Name

SSLPassPhraseDialog

Default Value

API Name

passphrasefile_location

Required

false

Hue Load Balancer TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Hue Load Balancer is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

SSLCertificateFile

Default Value

API Name

ssl_certificate

Required

false

Hue Load Balancer TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Hue Load Balancer is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

SSLCertificateKeyFile

Default Value

API Name

ssl_certificate_key

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hue Load Balancer Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Load Balancer Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_log_dir

Required

true

Suppress Parameter Validation: Load Balancer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Load Balancer Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_role_env_safety_valve

Required

true

Suppress Parameter Validation: Load Balancer Advanced Configuration Snippet (Safety Valve) for httpd.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Load Balancer Advanced Configuration Snippet (Safety Valve) for httpd.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_safety_valve

Required

true

Suppress Parameter Validation: Hue Load Balancer Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Load Balancer Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_listen

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog parameter.

Related Name

Default Value

false

API Name

role_config_suppression_passphrasefile_location

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Hue Load Balancer TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Load Balancer TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_certificate

Required

true

Suppress Parameter Validation: Hue Load Balancer TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Load Balancer TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_certificate_key

Required

true

Suppress Parameter Validation: SSLCipherSuite

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSLCipherSuite parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_cipher_suite

Required

true

Suppress Parameter Validation: SSLProtocol

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSLProtocol parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_protocol

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hue_load_balancer_unexpected_exits

Required

true

Service-Wide

Advanced

Enable Django Debug Mode

Description

In debug mode, Django displays a detailed traceback when an exception occurs. Debugging information may contain sensitive data. Django remembers every SQL query it executes in debug mode, which will rapidly consume memory.

Related Name

django_debug_mode

Default Value

false

API Name

django_debug_enable

Required

false

Enable Debugging of Internal Server Error Responses

Description

Enable debug output in HTTP Internal Server Error (status 500) responses. Debugging information may contain sensitive data. If Enable Django Debug Mode is set, this is automatically enabled.

Related Name

http_500_debug_mode

Default Value

false

API Name

http_500_debug_enable

Required

false

Hue Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hue_service_env_safety_valve

Required

false

Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini

Description

For advanced use only, a string to be inserted into hue_safety_valve.ini. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

hue_service_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hue

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hue

API Name

process_username

Required

true

Enable Usage Data Collection

Description

When you enable anonymous usage data collection Hue tracks anonymised pages and application versions in order to gather information about each application's usage levels. The data collected does not include any hostnames or IDs. Data collection option is available on CDH 4.4 and later deployments.

Related Name

collect_usage

Default Value

true

API Name

usage_data_collection_enable

Required

false

Cloudera Navigator Optimizer

Auto Upload Queries to Cloudera Navigator Optimizer

Description

Automatically upload queries after their execution in order to improve recommendations.

Related Name

auto_upload_queries

Default Value

true

API Name

auto_upload_queries

Required

false

Enable Cloudera Navigator Optimizer integration with Hue

Description

Enable Cloudera Navigator Optimizer integration with Hue.

Related Name

enable_navopt

Default Value

false

API Name

enable_navopt

Required

false

Cloudera Altus Access Key

Description

Credentials for accessing Cloudera cloud services.

Related Name

Default Value

API Name

navopt_altus_account

Required

false

Query History Upload Limit

Description

Allow admins to upload the last N executed queries in the quick start wizard. Use 0 to disable.

Related Name

query_history_upload_limit

Default Value

10000

API Name

query_history_upload_limit

Required

false

Database

Hue Database Directory

Description

If the database is SQLite3, this is the filename of the database to use, and the directory of this file must be writable by the 'hue' user.

Related Name

dir

Default Value

/var/lib/hue/desktop.db

API Name

database_dir

Required

false

Database Dump File

Description

File where the database gets dumped to or loaded from.

Related Name

Default Value

/tmp/hue_database_dump.json

API Name

database_dump_file

Required

true

Hue Database Hostname

Description

Name of host where the Hue database is running. Not necessary for SQLite3.

Related Name

host

Default Value

localhost

API Name

database_host

Required

false

Hue Database Name

Description

Name of Hue database.

Related Name

name

Default Value

hue

API Name

database_name

Required

false

Hue Database Password

Description

Password for Hue database. Not necessary for SQLite3.

Related Name

password

Default Value

API Name

database_password

Required

false

Hue Database Port

Description

Port on host where the Hue database is running. Not necessary for SQLite3.

Related Name

port

Default Value

3306

API Name

database_port

Required

false

Hue Database Type

Description

Type of database used for Hue

Related Name

engine

Default Value

sqlite3

API Name

database_type

Required

false

Hue Database Username

Description

The username to use to log into the Hue database. Not necessary for SQLite3.

Related Name

user

Default Value

hue

API Name

database_user

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Hue Server Monitoring Thresholds

Description

The health test thresholds of the overall Hue Server health. The check returns "Concerning" health if the percentage of "Healthy" Hue Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Hue Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hue_hue_servers_healthy_thresholds

Required

false

Healthy Kerberos Ticket Renewer Monitoring Thresholds

Description

The health test thresholds of the overall Kerberos Ticket Renewer health. The check returns "Concerning" health if the percentage of "Healthy" Kerberos Ticket Renewers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kerberos Ticket Renewers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hue_kt_renewers_healthy_thresholds

Required

false

Healthy Load Balancer Monitoring Thresholds

Description

The health test thresholds of the overall Load Balancer health. The check returns "Concerning" health if the percentage of "Healthy" Load Balancers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Load Balancers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

hue_load_balancer_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.

- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Atlas Service

Description

Name of the Atlas service that this Hue service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Blacklist

Description

Comma-separated list of regular expressions, which match any prefix of 'host:port/path' of requested proxy target. This does not support matching GET parameters.

Related Name

blacklist

Default Value

()

API Name

blacklist

Required

false

Hue Web Server Threads

Description

Number of threads used by the Hue web server.

Related Name

cherrypy_server_threads

Default Value

50

API Name

cherrypy_server_threads

Required

false

Default Site Encoding

Description

Default encoding for site data.

Related Name

default_site_encoding

Default Value

utf

API Name

default_site_encoding

Required

false

Default User Group

Description

The name of a default group that users will be added to at creation time.

Related Name

default_user_group

Default Value

API Name

default_user_group

Required

false

HBase Service

Description

Name of the HBase service that this Hue service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

false

HDFS Service

Description

Name of the HDFS service that this Hue service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

HDFS Temporary Directory

Description

HDFS directory used for storing temporary files.

Related Name

temp_dir

Default Value

/tmp

API Name

hdfs_tmp_dir

Required

false

HiveServer2 Service

Description

Name of the HiveServer2 service that this Hue service instance depends on

Related Name

Default Value

API Name

hive_service

Required

false

HMS Service

Description

Name of the HMS service that this Hue service instance depends on

Related Name

Default Value

API Name

hms_service

Required

true

Hue Kerberos Credentials Cache Directory

Description

Directory where Hue stores cached Kerberos credentials

Related Name

ccache_path

Default Value

/var/run/hue

API Name

hue_ccache_path

Required

false

HBase Thrift Server

Description

Thrift server to use for HBase app.

Related Name

Default Value

API Name

hue_hbase_thrift

Required

false

HDFS Web Interface Role

Description

HTTPFS role or Namenode (if webhdfs is enabled) that hue can use to communicate with HDFS.

Related Name

webhdfs_url

Default Value

API Name

hue_webhdfs

Required

false

Impala Service

Description

Name of the Impala service that this Hue service instance depends on

Related Name

Default Value

API Name

impala_service

Required

false

Knox Proxy Hosts

Description

List of hosts that Knox proxy requests can come from.

Related Name

knox_proxyhosts

Default Value

API Name

knox_proxyhosts

Required

false

Oozie Service

Description

Name of the Oozie service that this Hue service instance depends on

Related Name

Default Value

API Name

oozie_service

Required

false

Solr Service

Description

Name of the Solr service that this Hue service instance depends on

Related Name

Default Value

API Name

solr_service

Required

false

Time Zone

Description

Time zone name.

Related Name

time_zone

Default Value

America/Los_Angeles

API Name

time_zone

Required

false

User Augmentor

Description

Class that defines extra accessor methods for user objects.

Related Name

user_augmentor

Default Value

desktop.auth.backend.DefaultUserAugmentor

API Name

user_augmentor

Required

false

Whitelist

Description

Comma-separated list of regular expressions, which match 'host:port' of requested proxy target.

Related Name

whitelist

Default Value

(localhost|127\.0\.0\.1):(50030|50070|50060|50075)

API Name

whitelist

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Hue service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Security

Authentication Backend

Description

Mode of authenticating login credentials. Select desktop.auth.backend.LdapBackend to use LDAP to authenticate login credentials. LDAP requires you to also set the LDAP URL, Active Directory Domain, and optionally LDAP certificate if you are using secure LDAP. Select desktop.auth.backend.PamBackend to use PAM to authenticate login credentials.

Related Name

backend

Default Value

desktop.auth.backend.AllowFirstUserDjangoBackend

API Name

auth_backend

Required

false

LDAP Search Base

Description

The distinguished name to use as a search base for finding users and groups. This should be similar to 'dc=hadoop,dc=mycompany,dc=com'.

Related Name

base_dn

Default Value

API Name

base_dn

Required

false

LDAP Bind User Distinguished Name

Description

Distinguished name of the user to bind to AD as for user authentication search/bind and group lookup for role authorization. For openLDAP based directories this should be a DN string, for Active Directory this can be just a username, combined with the "Active Directory Domain" value for login. For example username in the field and example.com in the active directory domain will result in the User Principal Name value of username@example.com being used to bind. If you put a UPM value here, do not over-configure the "active directory domain" field otherwise you will end up presenting username@example.com@example.com for binds. AD will accept a UPN value or the DN value as a valid Bind DN; An example of a Distinguished Name (DN): CN=cdh admin,OU=svcaccount,DC=example,DC=com An example of a UPN value: cdhadmin@example.com

Related Name

bind_dn

Default Value

API Name

bind_dn

Required

false

LDAP Bind Password

Description

The password of the bind user.

Related Name

bind_password

Default Value

API Name

bind_password

Required

false

Create LDAP users on login

Description

Create users in Hue when they try to login with their LDAP credentials. For use when using LdapBackend for Hue authentication.

Related Name

create_users_on_login

Default Value

true

API Name

create_users_on_login

Required

false

LDAP Group Filter

Description

Base filter for searching for groups. For Active Directory, this is typically '(objectClass=group)'.

Related Name

group_filter

Default Value

API Name

group_filter

Required

false

LDAP Group Membership Attribute

Description

The attribute of the group object that identifies the members of the group. For Active Directory, this is typically 'member'.

Related Name

group_member_attr

Default Value

API Name

group_member_attr

Required

false

LDAP Group Name Attribute

Description

The group name attribute in the LDAP schema. For Active Directory, this is typically 'cn'.

Related Name

group_name_attr

Default Value

API Name

group_name_attr

Required

false

Auto Logout Timeout

Description

Auto logout/idle session timeout in seconds, -1 second is equivalent to no automatic logout.

Related Name

idle_session_timeout

Default Value

-1 second(s)

API Name

idle_session_timeout

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hue

API Name

kerberos_princ_name

Required

true

LDAP Server CA Certificate

Description

The location on disk of the certificate, in .pem format, used to confirm the authenticity of the LDAP server certificate. This is the Certificate Authority (CA) certificate, and it was used to sign the LDAP server certificate. If not set, all certificates are trusted, which means that an attacker could potentially intercept otherwise encrypted usernames and passwords.

Related Name

ldap_cert

Default Value

API Name

ldap_cert

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

ldap_url

Default Value

API Name

ldap_url

Required

false

LDAP Username Pattern

Description

LDAP Username Pattern for use with non-Active Directory LDAP implementations. Must contain the special '*username*' string for replacement during authentication.

Related Name

ldap_username_pattern

Default Value

API Name

ldap_username_pattern

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

nt_domain

Default Value

API Name

nt_domain

Required

false

PAM Backend Service Name

Description

The PAM service name to use when authenticating over desktop.auth.backend.PamBackend. This is typically the name of a file under /etc/pam.d/ on the Hue host.

Related Name

pam_service

Default Value

login

API Name

pam_auth_service

Required

false

Use Search Bind Authentication

Description

Search Bind Authentication connects to the LDAP server using credentials provided in the 'bind_dn' and 'bind_password' configurations. If these configurations are not set, then an anonymous search is performed.

Related Name

search_bind_authentication

Default Value

false

API Name

search_bind_authentication

Required

false

LDAP Group Name for Test LDAP Configuration

Description

An optional group name for validating LDAP group configurations. If a test group name is provided, Hue's LDAP library uses it as a search parameter when running the command, Test Hue LDAP Configuration (under Hue * Actions). For example, (&(objectClass=*) (sAMAccountName=test_ldap_group)). If test group name is not provided then Hue LDAP Configuration action will check only LDAP server connectivity.

Related Name

test_ldap_group

Default Value

API Name

test_ldap_group

Required

false

LDAP Username for Test LDAP Configuration

Description

An optional user name for validating LDAP user configurations. If a test user name is provided, Hue's LDAP library uses it as a search parameter when running the command,

Test Hue LDAP Configuration (under Hue * Actions). For example, (&(objectClass=*)(sAMAccountName=test_ldap_user)). If "*" is provided, then all user attributes are returned. If test user name is not provided then Test Hue LDAP Configuration action will check only LDAP server connectivity.

Related Name

test_ldap_user

Default Value

API Name

test_ldap_user

Required

false

Enable LDAP TLS

Description

If true, attempts to establish a TLS (Transport Layer Security) connection with an LDAP server that was specified with ldap://. Not required when using an LDAP URL with prefix ldaps://, because that already specifies TLS. This option is also known as "Use StartTLS".

Related Name

use_start_tls

Default Value

true

API Name

use_start_tls

Required

false

LDAP User Filter

Description

The base filter for searching for users. For Active Directory, this is typically '(objectClass=user)'.

Related Name

user_filter

Default Value

API Name

user_filter

Required

false

LDAP Username Attribute

Description

The username attribute in the LDAP schema. For Active Directory, this is typically 'sAMAccountName'.

Related Name

user_name_attr

Default Value

API Name

user_name_attr

Required

false

Suppressions

Suppress Configuration Validator: Top Banner Custom HTML

Description

Whether to suppress configuration warnings produced by the Top Banner Custom HTML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_banner_html

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Hue HTTP Port

Description

Whether to suppress configuration warnings produced by the Hue HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_http_port

Required

true

Suppress Configuration Validator: Hue Server Advanced Configuration Snippet (Safety Valve) for impalad_flags

Description

Whether to suppress configuration warnings produced by the Hue Server Advanced Configuration Snippet (Safety Valve) for impalad_flags configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_impalad_flags_safety_valve

Required

true

Suppress Configuration Validator: Hue Load Balancer Log Directory

Description

Whether to suppress configuration warnings produced by the Hue Load Balancer Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_log_dir

Required

true

Suppress Configuration Validator: Load Balancer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Load Balancer Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_role_env_safety_valve

Required

true

Suppress Configuration Validator: Load Balancer Advanced Configuration Snippet (Safety Valve) for httpd.conf

Description

Whether to suppress configuration warnings produced by the Load Balancer Advanced Configuration Snippet (Safety Valve) for httpd.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_load_balancer_safety_valve

Required

true

Suppress Configuration Validator: Metrics Sample File Location

Description

Whether to suppress configuration warnings produced by the Metrics Sample File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_metrics_sample_file_location

Required

true

Suppress Configuration Validator: Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml

Description

Whether to suppress configuration warnings produced by the Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_hive_safety_valve

Required

true

Suppress Configuration Validator: Hue Server Advanced Configuration Snippet (Safety Valve) for hue_safety_valve_server.ini

Description

Whether to suppress configuration warnings produced by the Hue Server Advanced Configuration Snippet (Safety Valve) for hue_safety_valve_server.ini configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_hue_safety_valve

Required

true

Suppress Configuration Validator: Hue Server Log Directory

Description

Whether to suppress configuration warnings produced by the Hue Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_log_dir

Required

true

Suppress Configuration Validator: Jobsub Examples and Templates Directory

Description

Whether to suppress configuration warnings produced by the Jobsub Examples and Templates Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_remote_data_dir

Required

true

Suppress Configuration Validator: Hue Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Hue Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Hue Server Safety Valve Format Validator

Description

Whether to suppress configuration warnings produced by the Hue Server Safety Valve Format Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_server_safety_valve_format_validator

Required

true

Suppress Configuration Validator: Hue Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties

Description

Whether to suppress configuration warnings produced by the Hue Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_sqoop2_properties_safety_valve

Required

true

Suppress Configuration Validator: Hue TLS/SSL Validator

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hue_ssl_validator

Required

true

Suppress Configuration Validator: Kerberos Ticket Renewer Log Directory

Description

Whether to suppress configuration warnings produced by the Kerberos Ticket Renewer Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kt_renewer_log_dir

Required

true

Suppress Configuration Validator: Kerberos Ticket Renewer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Kerberos Ticket Renewer Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kt_renewer_role_env_safety_valve

Required

true

Suppress Configuration Validator: Hue Load Balancer Port

Description

Whether to suppress configuration warnings produced by the Hue Load Balancer Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_listen

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog

Description

Whether to suppress configuration warnings produced by the Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_passphrasefile_location

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Secret Key

Description

Whether to suppress configuration warnings produced by the Secret Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secret_key

Required

true

Suppress Configuration Validator: Hue TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Server CA Certificate (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_cacerts

Required

true

Suppress Configuration Validator: Hue TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_certificate

Required

true

Suppress Configuration Validator: Hue Load Balancer TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Hue Load Balancer TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_certificate_key

Required

true

Suppress Configuration Validator: SSLCipherSuite

Description

Whether to suppress configuration warnings produced by the SSLCipherSuite configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_cipher_suite

Required

true

Suppress Configuration Validator: Hue TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_private_key

Required

true

Suppress Configuration Validator: Hue TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Hue TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_private_key_password

Required

true

Suppress Configuration Validator: SSLProtocol

Description

Whether to suppress configuration warnings produced by the SSLProtocol configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_protocol

Required

true

Suppress Parameter Validation: LDAP Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Search Base parameter.

Related Name

Default Value

false

API Name

service_config_suppression_base_dn

Required

true

Suppress Parameter Validation: LDAP Bind User Distinguished Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind User Distinguished Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_bind_dn

Required

true

Suppress Parameter Validation: LDAP Bind Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_bind_password

Required

true

Suppress Parameter Validation: Blacklist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Blacklist parameter.

Related Name

Default Value

false

API Name

service_config_suppression_blacklist

Required

true

Suppress Parameter Validation: Hue Database Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_dir

Required

true

Suppress Parameter Validation: Database Dump File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Dump File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_dump_file

Required

true

Suppress Parameter Validation: Hue Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Hostname parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_host

Required

true

Suppress Parameter Validation: Hue Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_name

Required

true

Suppress Parameter Validation: Hue Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_password

Required

true

Suppress Parameter Validation: Hue Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_port

Required

true

Suppress Parameter Validation: Hue Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Database Username parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_user

Required

true

Suppress Parameter Validation: Default Site Encoding

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Site Encoding parameter.

Related Name

Default Value

false

API Name

service_config_suppression_default_site_encoding

Required

true

Suppress Parameter Validation: Default User Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default User Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_default_user_group

Required

true

Suppress Parameter Validation: LDAP Group Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_group_filter

Required

true

Suppress Parameter Validation: LDAP Group Membership Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Membership Attribute parameter.

Related Name

Default Value

false

API Name

service_config_suppression_group_member_attr

Required

true

Suppress Parameter Validation: LDAP Group Name Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Name Attribute parameter.

Related Name

Default Value

false

API Name

service_config_suppression_group_name_attr

Required

true

Suppress Configuration Validator: HDFS HTTPFS Usage Validator

Description

Whether to suppress configuration warnings produced by the HDFS HTTPFS Usage Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_httpfs_present_validator

Required

true

Suppress Parameter Validation: HDFS Temporary Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Temporary Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_tmp_dir

Required

true

Suppress Parameter Validation: Hue Kerberos Credentials Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Kerberos Credentials Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_ccache_path

Required

true

Suppress Configuration Validator: HBase Thrift Usage Validator

Description

Whether to suppress configuration warnings produced by the HBase Thrift Usage Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_hbase_thrift_server_validator

Required

true

Suppress Configuration Validator: Knox Proxy Hosts validator for Hue

Description

Whether to suppress configuration warnings produced by the Knox Proxy Hosts validator for Hue configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_knox_proxyhosts_validator

Required

true

Suppress Configuration Validator: Load Balancer Count Validator

Description

Whether to suppress configuration warnings produced by the Load Balancer Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_load_balancer_count_validator

Required

true

Suppress Configuration Validator: Phoenix Query Server

Description

Whether to suppress configuration warnings produced by the Phoenix Query Server configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_phoenix_query_server_validator

Required

true

Suppress Configuration Validator: Hue Server Count Validator

Description

Whether to suppress configuration warnings produced by the Hue Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_server_count_validator

Required

true

Suppress Configuration Validator: Hue Service Config Safety Valve Format Validator

Description

Whether to suppress configuration warnings produced by the Hue Service Config Safety Valve Format Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hue_service_config_safety_valve_format_validator

Required

true

Suppress Parameter Validation: Hue Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_service_env_safety_valve

Required

true

Suppress Parameter Validation: Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_service_safety_valve

Required

true

Suppress Parameter Validation: HDFS Web Interface Role

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Web Interface Role parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hue_webhdfs

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Knox Proxy Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_proxyhosts

Required

true

Suppress Configuration Validator: Kerberos Ticket Renewer Count Validator

Description

Whether to suppress configuration warnings produced by the Kerberos Ticket Renewer Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kt_renewer_count_validator

Required

true

Suppress Parameter Validation: LDAP Server CA Certificate

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Server CA Certificate parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_cert

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_url

Required

true

Suppress Parameter Validation: LDAP Username Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Username Pattern parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_username_pattern

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_nt_domain

Required

true

Suppress Parameter Validation: PAM Backend Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the PAM Backend Service Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_pam_auth_service

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: LDAP Group Name for Test LDAP Configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Name for Test LDAP Configuration parameter.

Related Name

Default Value

false

API Name

service_config_suppression_test_ldap_group

Required

true

Suppress Parameter Validation: LDAP Username for Test LDAP Configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Username for Test LDAP Configuration parameter.

Related Name

Default Value

false

API Name

service_config_suppression_test_ldap_user

Required

true

Suppress Parameter Validation: Time Zone

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Time Zone parameter.

Related Name

Default Value

false

API Name

service_config_suppression_time_zone

Required

true

Suppress Parameter Validation: User Augmentor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the User Augmentor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_user_augmentor

Required

true

Suppress Parameter Validation: LDAP User Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_user_filter

Required

true

Suppress Parameter Validation: LDAP Username Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Username Attribute parameter.

Related Name

Default Value

false

API Name

service_config_suppression_user_name_attr

Required

true

Suppress Parameter Validation: Whitelist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Whitelist parameter.

Related Name

Default Value

false

API Name

service_config_suppression_whitelist

Required

true

Suppress Health Test: Hue Server Health

Description

Whether to suppress the results of the Hue Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hue_hue_servers_healthy

Required

true

Suppress Health Test: Kerberos Ticket Renewer Health

Description

Whether to suppress the results of the Kerberos Ticket Renewer Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hue_kt_renewers_healthy

Required

true

Suppress Health Test: Load Balancer Health

Description

Whether to suppress the results of the Load Balancer Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_hue_load_balancer_healthy

Required

true

Iceberg Replication Properties in Cloudera Runtime 7.2.18

Role groups:

Admin Server

Advanced

Admin Server Advanced Configuration Snippet (Safety Valve) for iceberg_replication.xml

Description

For advanced use only. A string to be inserted into iceberg_replication.xml for this role only.

Related Name

Default Value

API Name

iceberg_replication.xml_role_safety_valve

Required

false

Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

ICEBERG_REPLICATION_ADMINSERVER_role_env_safety_valve

Required

false

Admin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j2.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value
20

API Name
process_start_secs

Required
false

Logs

Admin Server Log Directory

Description
The log directory for log files of the role Admin Server.

Related Name
log_dir

Default Value
/var/log/iceberg_replication/admin_server

API Name
log_dir

Required
false

Admin Server Logging Threshold

Description
The minimum log level for Admin Server logs

Related Name

Default Value
INFO

API Name
log_threshold

Required
false

Admin Server Maximum Log File Backups

Description
The maximum number of rolled log files to keep for Admin Server logs. Typically used by log4j or logback.

Related Name

Default Value
10

API Name
max_log_backup_index

Required
false

Admin Server Max Log Size

Description

The maximum size, in megabytes, per log file for Admin Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

iceberg_replication_adminserver_fd_thresholds

Required

false

Admin Server Host Health Test

Description

When computing the overall Admin Server health, consider the host's health.

Related Name

Default Value

true

API Name

iceberg_replication_adminserver_host_health_enabled

Required

false

Admin Server Process Health Test

Description

Enables the health test that the Admin Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

iceberg_replication_adminserver_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.

- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Admin Server Port Number

Description

The port number on which admin server runs

Related Name

admin_server_port_number

Default Value

2288

API Name

admin_server_port_number

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Admin Server Port Number

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Port Number parameter.

Related Name

Default Value

false

API Name

role_config_suppression_admin_server_port_number

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Admin Server Advanced Configuration Snippet (Safety Valve) for iceberg_replication.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Advanced Configuration Snippet (Safety Valve) for iceberg_replication.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_iceberg_replication.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_iceberg_replication_adminserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Admin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Admin Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_iceberg_replication_iceberg_replication_adminserver_unexpected_exits

Required

true

Service-Wide

Advanced

Iceberg Replication Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ICEBERG_REPLICATION_service_env_safety_valve

Required

false

Advanced log4j properties for "export" step of iceberg replication.

Description

Add log4j properties that will be referred by "export" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_export

Required

false

Advanced log4j properties for "get checkpoint" names step of iceberg replication.

Description

Add log4j properties that will be referred by "get checkpoint" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_get_checkpoint

Required

false

Advanced log4j properties for "get identity" step of iceberg replication.

Description

Add log4j properties that will be referred by "get identity" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_get_idenity

Required

false

Advanced log4j properties for "get table names" step of iceberg replication.

Description

Add log4j properties that will be referred by "get table names" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_get_table_names

Required

false

Advanced log4j properties for "set origin" step of iceberg replication.

Description

Add log4j properties that will be referred by "set origin" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_set_origin

Required

false

Advanced log4j properties for "sync" step of iceberg replication.

Description

Add log4j properties that will be referred by "sync" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_sync

Required

false

Advanced log4j properties for "transfer(distcp)" step of iceberg replication.

Description

Add log4j properties that will be referred by "transfer(distcp)" step of iceberg replication. Property added here will be appended in the log4j.properties file generated in run directory of this step.

Related Name

Default Value

API Name

log4j_safety_valve_for_xfer

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HDFS Service

Description

Name of the HDFS service that this Iceberg Replication service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

HMS Service

Description

Name of the HMS service that this Iceberg Replication service instance depends on

Related Name

Default Value

API Name

hms_service

Required

true

Iceberg Replication HDFS Directory

Description

The HDFS user directory for Iceberg Replication.

Related Name

iceberg_replication_hdfs_dir

Default Value

/user/iceberg_replication

API Name

iceberg_replication_hdfs_dir

Required

true

Advanced command line options for distcp used in Iceberg Replication.

Description

Add command line option(s) to the distcp invocation of Iceberg Replication. Separate command line options with a space. These options will be appended to all distcp invocations during Iceberg Replication by all policies.

Related Name

Default Value

API Name

iceberg_replication_safety_valve_for_xfer_options

Required

false

YARN Service

Description

Name of the YARN service that this Iceberg Replication service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

Suppressions

Suppress Configuration Validator: Admin Server Port Number

Description

Whether to suppress configuration warnings produced by the Admin Server Port Number configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_admin_server_port_number

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Admin Server Advanced Configuration Snippet (Safety Valve) for iceberg_replication.xml

Description

Whether to suppress configuration warnings produced by the Admin Server Advanced Configuration Snippet (Safety Valve) for iceberg_replication.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_iceberg_replication.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Admin Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_iceberg_replication_adminserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Admin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Admin Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Admin Server Log Directory

Description

Whether to suppress configuration warnings produced by the Admin Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Admin Server Count Validator

Description

Whether to suppress configuration warnings produced by the Admin Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_iceberg_replication_adminserver_count_validator

Required

true

Suppress Parameter Validation: Iceberg Replication HDFS Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Iceberg Replication HDFS Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_iceberg_replication_hdfs_dir

Required

true

Suppress Parameter Validation: Advanced command line options for distcp used in Iceberg Replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced command line options for distcp used in Iceberg Replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_iceberg_replication_safety_valve_for_xfer_options

Required

true

Suppress Parameter Validation: Iceberg Replication Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Iceberg Replication Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_iceberg_replication_service_env_safety_valve

Required

true

Suppress Parameter Validation: Advanced log4j properties for "export" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "export" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_export

Required

true

Suppress Parameter Validation: Advanced log4j properties for "get checkpoint" names step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "get checkpoint" names step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_get_checkpoint

Required

true

Suppress Parameter Validation: Advanced log4j properties for "get identity" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "get identity" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_get_idenity

Required

true

Suppress Parameter Validation: Advanced log4j properties for "get table names" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "get table names" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_get_table_names

Required

true

Suppress Parameter Validation: Advanced log4j properties for "set origin" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "set origin" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_set_origin

Required

true

Suppress Parameter Validation: Advanced log4j properties for "sync" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "sync" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_sync

Required

true

Suppress Parameter Validation: Advanced log4j properties for "transfer(distcp)" step of iceberg replication.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced log4j properties for "transfer(distcp)" step of iceberg replication. parameter.

Related Name

Default Value

false

API Name

service_config_suppression_log4j_safety_valve_for_xfer

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Impala Properties in Cloudera Runtime 7.2.18

Role groups:

Impala Catalog Server

Advanced

Catalog Server Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to Catalog Server command line flags. Key names should begin with a hyphen(-). For example: -log_filename=foo.log

Related Name

Default Value

API Name

catalogd_cmd_args_safety_valve

Required

false

Impala Catalog Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

catalogd_core_site_safety_valve

Required

false

Catalog Server HBase Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

catalogd_hbase_conf_safety_valve

Required

false

Catalog Server HDFS Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

catalogd_hdfs_site_conf_safety_valve

Required

false

Catalog Server Hive Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

catalogd_hive_conf_safety_valve

Required

false

Java Configuration Options for Catalog Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

catalogd_java_opts

Required

false

Impala Catalog Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

CATALOGSERVER_role_env_safety_valve

Required

false

Catalog Server Core Dump Directory

Description

Directory where the Catalog Server core dump is placed.

Related Name

core_dump_dir

Default Value

/var/log/catalogd

API Name

core_dump_dir

Required

false

Catalog Server Hive Metastore Connection Retries

Description

Number of retry attempts the Catalog Server will make when connecting to the Hive Metastore Server. By default, the Catalog Server waits one second between retries.

Related Name

hive.metastore.connect.retries

Default Value

5

API Name

hive_metastore_connect_retries

Required

false

Catalog Server Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server from Catalog Server. Consider increasing this if you have tables with a lot of metadata and see timeout errors.

Related Name

hive.metastore.client.socket.timeout

Default Value

1 hour(s)

API Name

hive_metastore_timeout

Required

false

Metastore Notification Polling Interval

Description

The value of this configuration determines the interval with which the Catalog Server fetches new notifications from Hive Metastore. The feature is disabled when it is set to 0.

Related Name

hms_event_polling_interval_s

Default Value

2 second(s)

API Name

hms_event_polling_interval_s

Required

false

Load Catalog in Background

Description

If true, loads catalog metadata in the background. If false, metadata is loaded lazily (on access). Only effective in CDH 5 and Impala 1.2.4 and higher.

Related Name

load_catalog_in_background

Default Value

false

API Name

load_catalog_in_background

Required

false

Catalog Server Max Breakpad Dump Files

Description

Maximum number of Breakpad dump files stored by Catalog Server Role.

Related Name

max_minidumps

Default Value

9

API Name

max_minidumps

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Catalog Server Breakpad Dump Directory

Description

Directory for storing Catalog Server Breakpad dumps.

Related Name

minidump_path

Default Value

/var/log/impala-minidumps

API Name

minidump_path

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Catalog Server Log Directory

Description

Directory where Catalog Server will place its log files.

Related Name

log_dir

Default Value

/var/log/catalogd

API Name

log_dir

Required

false

Impala Catalog Server Logging Threshold

Description

The minimum log level for Impala Catalog Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Catalog Server Verbose Log Level

Description

Verbose logging level for the GLog logger. These messages are always logged at 'INFO' log level, so this setting has no effect if Logging Threshold is set to 'WARN' or above.

Related Name

GLOG_v

Default Value

1

API Name

log_verbose_level

Required

false

Catalog Server Log Buffer Level

Description

Buffer log messages logged at this level or lower (-1 means don't buffer; 0 means buffer INFO only; 1 means buffer WARNING only, ...)

Related Name

logbuflevel

Default Value

0

API Name

logbuflevel

Required

false

Catalog Server Maximum Log Files

Description

The number of log files that are kept for each severity level before all older log files are removed. The number has to be greater than 1 to keep at least the current log file open. If set to 0, all log files are retained and log rotation is effectively disabled.

Related Name

max_log_files

Default Value

10

API Name

max_log_files

Required

false

Impala Catalog Server Max Log Size

Description

The maximum size, in megabytes, per log file for Impala Catalog Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Catalog Server Connectivity Health Test

Description

Enables the health test that verifies the Catalog Server is connected to the StateStore

Related Name

Default Value

true

API Name

catalogserver_connectivity_health_enabled

Required

false

Catalog Server Connectivity Tolerance at Startup

Description

The amount of time to wait for the Catalog Server to fully start up and connect to the StateStore before enforcing the connectivity check.

Related Name

Default Value

3 minute(s)

API Name

catalogserver_connectivity_tolerance

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

catalogserver_fd_thresholds

Required

false

Impala Catalog Server Host Health Test

Description

When computing the overall Impala Catalog Server health, consider the host's health.

Related Name

Default Value

true

API Name

catalogserver_host_health_enabled

Required

false

Impala Catalog Server Process Health Test

Description

Enables the health test that the Impala Catalog Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

catalogserver_scm_health_enabled

Required

false

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Related Name

Default Value

5 minute(s)

API Name

catalogserver_startup_tolerance

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

catalogserver_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

catalogserver_web_metric_collection_thresholds

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The

follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify

$INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_resident_set_size_thresholds

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Catalog Server Web Server

Description

Enable/Disable Catalog Server web server. This web server contains useful information about Catalog Server daemon.

Related Name

enable_webserver

Default Value

true

API Name

catalogd_enable_webserver

Required

false

Force the Catalog Server active

Description

Force the Catalog Server to be always active under HA mode if it is online.

Related Name

force_catalogd_active

Default Value

false

API Name

force_catalogd_active

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Catalog Server Service Port

Description

Port where Catalog Server is exported.

Related Name

catalog_service_port

Default Value

26000

API Name

catalog_service_port

Required

false

Catalog Server HTTP Server Port

Description

Port where Catalog Server debug web server runs.

Related Name

webserver_port

Default Value

25020

API Name

catalogserver_webserver_port

Required

false

Resource Management

Java Heap Size of Catalog Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

4 GiB

API Name

catalogd_embedded_jvm_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Catalog Server Webserver TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Catalog Server Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_certificate_file

Default Value

API Name

webserver_certificate_file

Required

false

Catalog Server Web Server User Password

Description

Password for Catalog Server web server authentication.

Related Name

webserver_htpassword_password

Default Value

API Name

webserver_htpassword_password

Required

false

Catalog Server Web Server Username

Description

Username for Catalog Server web server authentication.

Related Name

webserver_htpassword_user

Default Value

API Name

webserver_htpassword_user

Required

false

Catalog Server Webserver TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Catalog Server Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_private_key_file

Default Value

API Name

webserver_private_key_file

Required

false

Catalog Server Webserver TLS/SSL Private Key Password

Description

The password for the private key in the Catalog Server Webserver TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

webserver_private_key_password_cmd

Default Value

API Name

webserver_private_key_password_cmd

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Catalog Server Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalog_service_port

Required

true

Suppress Parameter Validation: Catalog Server Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Command Line Argument Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_cmd_args_safety_valve

Required

true

Suppress Parameter Validation: Impala Catalog Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Catalog Server Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_core_site_safety_valve

Required

true

Suppress Parameter Validation: Catalog Server HBase Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server HBase Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hbase_conf_safety_valve

Required

true

Suppress Parameter Validation: Catalog Server HDFS Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server HDFS Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hdfs_site_conf_safety_valve

Required

true

Suppress Parameter Validation: Catalog Server Hive Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Hive Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hive_conf_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for Catalog Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Catalog Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_java_opts

Required

true

Suppress Parameter Validation: Impala Catalog Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Catalog Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: Catalog Server HTTP Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server HTTP Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_catalogserver_webserver_port

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Catalog Server Core Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Core Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_dump_dir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Catalog Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Catalog Server Breakpad Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Breakpad Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_minidump_path

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Catalog Server Webserver TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Webserver TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_certificate_file

Required

true

Suppress Parameter Validation: Catalog Server Web Server User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Web Server User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_password

Required

true

Suppress Parameter Validation: Catalog Server Web Server Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Web Server Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_user

Required

true

Suppress Parameter Validation: Catalog Server Webserver TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Webserver TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_file

Required

true

Suppress Parameter Validation: Catalog Server Webserver TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Catalog Server Webserver TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_password_cmd

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_audit_health

Required

true

Suppress Health Test: StateStore Connectivity

Description

Whether to suppress the results of the StateStore Connectivity heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_connectivity

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_log_directory_free_space

Required

true

Suppress Health Test: Resident Set Size

Description

Whether to suppress the results of the Resident Set Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_memory_rss_health

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_otelcol_health

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_catalogserver_web_metric_collection

Required

true

Impala Daemon

Advanced

Abort on Config Error

Description

Abort Impala startup if there are improper configs or running on unsupported hardware.

Related Name

abort_on_config_error

Default Value

true

API Name

abort_on_config_error

Required

false

Impala Daemon Core Dump Directory

Description

Directory where an Impala Daemon core dump is placed.

Related Name

core_dump_dir

Default Value

/var/log/impalad

API Name

core_dump_dir

Required

false

Impala Daemon Max Client Connections

Description

Maximum number of concurrent client connections allowed. This determines how many queries can run simultaneously. When more clients try to connect to Impala than the value of this setting, the later arriving clients have to wait until previous clients disconnect. Setting this value too high could negatively impact query latency.

Related Name

fe_service_threads

Default Value

64

API Name

fe_service_threads

Required

false

Impala Daemon Hive Metastore Connection Retries

Description

Number of retry attempts the Impala Daemon will make when connecting to the Hive Metastore Server. By default, the Impala Daemon waits one second between retries.

Related Name

hive.metastore.connect.retries

Default Value

5

API Name

hive_metastore_connect_retries

Required

false

Impala Daemon Hive Metastore Connection Timeout

Description

Timeout for requests to the Hive Metastore Server from Impala. Consider increasing this if you have tables with a lot of metadata and see timeout errors.

Related Name

hive.metastore.client.socket.timeout

Default Value

1 hour(s)

API Name

hive_metastore_timeout

Required

false

Impala Daemon HDFS Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hdfs-site.xml for this role only.

Related Name

Default Value

API Name

impala_hdfs_site_conf_safety_valve

Required

false

Impala Daemon Hive Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hive-site.xml for this role only.

Related Name

Default Value

API Name

impala_hive_conf_safety_valve

Required

false

Impala Daemon Llama Site Advanced Configuration Snippet (Safety Valve)

Description

An XML snippet to append to llama-site.xml for Impala Daemons. This configuration only has effect on Impala versions 1.3 or greater.

Related Name

Default Value

API Name

impala_llama_site_conf_safety_valve

Required

false

Impala Daemon Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to Impala Daemon command-line flags. Key names should begin with a hyphen(-). For example: -log_filename=fo o.log

Related Name

Default Value

API Name

impalad_cmd_args_safety_valve

Required

false

Impala Daemon Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

impalad_core_site_safety_valve

Required

false

Java Configuration Options for Impala Daemon

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Impala Daemon Java Options

Default Value

API Name

impalad_embedded_java_opts

Required

false

Impala Daemon Fair Scheduler Advanced Configuration Snippet (Safety Valve)

Description

An XML string to use verbatim for the contents of fair-scheduler.xml for Impala Daemons. This configuration only has effect on Impala versions 1.3 or greater.

Related Name

Default Value

API Name

impalad_fair_scheduler_safety_valve

Required

false

Impala Daemon HBase Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into hbase-site.xml for this role only.

Related Name

Default Value

API Name

impalad_hbase_conf_safety_valve

Required

false

Result Cache Maximum Size

Description

Maximum number of query results a client may request to be cached on a per-query basis to support restarting fetches. This option guards against unreasonably large result caches requested by clients. Requests exceeding this maximum will be rejected.

Related Name

max_result_cache_size

Default Value

100000

API Name

impalad_result_cache_max_size

Required

false

Impala Daemon Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

IMPALAD_role_env_safety_valve

Required

false

Llama Maximum Request Attempts

Description

Maximum number of times a request to reserve, expand, or release resources is attempted until the request is cancelled.

Related Name

llama_max_request_attempts

Default Value

5

API Name

llama_max_request_attempts

Required

false

Llama Registration Timeout Seconds

Description

Maximum number of seconds that Impala attempts to register or re-register with Llama. If registration is unsuccessful, Impala cancels the action with an error, which could result in an impalad startup failure or a cancelled query. A setting of -1 seconds means try indefinitely.

Related Name

llama_registration_timeout_secs

Default Value

30 second(s)

API Name

llama_registration_timeout_secs

Required

false

Llama Registration Wait Seconds

Description

Number of seconds to wait between attempts during Llama registration.

Related Name

llama_registration_wait_secs

Default Value

3 second(s)

API Name

llama_registration_wait_secs

Required

false

Impala Daemon Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Impala Daemon Max Breakpad Dump Files

Description

Maximum number of Breakpad dump files stored by Impala Daemon Role.

Related Name

max_minidumps

Default Value

9

API Name

max_minidumps

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Impala Daemon Breakpad Dump Directory

Description

Directory for storing Impala Daemon Breakpad dumps.

Related Name

minidump_path

Default Value

/var/log/impala-minidumps

API Name

minidump_path

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Impala Daemon Audit Log Directory

Description

The directory in which Impala daemon audit event log files are written. If "Impala Audit Event Generation" property is enabled, Impala will generate its audit logs in this directory.

Related Name

audit_event_log_dir

Default Value

/var/log/impalad/audit

API Name

audit_event_log_dir

Required

true

Enable Impala Audit Event Generation

Description

Enables audit event generation by Impala daemons. The audit log file will be placed in the directory specified by 'Impala Daemon Audit Log Directory' parameter.

Related Name

enable_audit_event_log

Default Value

false

API Name

enable_audit_event_log

Required

false

Enable Impala Lineage Generation

Description

Enables lineage generation by Impala daemons. The lineage log file is placed in the directory specified by the 'Impala Daemon Lineage Log Directory' parameter.

Related Name

enable_lineage_log

Default Value

true

API Name

enable_lineage_log

Required

false

Impala Daemon Lineage Log Directory

Description

The directory in which Impala daemon lineage log files are written. If "Impala Lineage Generation" property is enabled, Impala generates its lineage logs in this directory.

Related Name

lineage_event_log_dir

Default Value

/var/log/impalad/lineage

API Name

lineage_event_log_dir

Required

true

Impala Daemon Log Directory

Description

Directory where Impala Daemon will place its log files.

Related Name

log_dir

Default Value

/var/log/impalad

API Name

log_dir

Required

false

Impala Daemon Logging Threshold

Description

The minimum log level for Impala Daemon logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Impala Daemon Verbose Log Level

Description

Verbose logging level for the GLog logger. These messages are always logged at 'INFO' log level, so this setting has no effect if Logging Threshold is set to 'WARN' or above.

Related Name

GLOG_v

Default Value

1

API Name

log_verbose_level

Required

false

Impala Daemon Log Buffer Level

Description

Buffer log messages logged at this level or lower (-1 means don't buffer; 0 means buffer INFO only; 1 means buffer WARNING only, ...)

Related Name

logbuflevel

Default Value

0

API Name

logbuflevel

Required

false

Impala Daemon Maximum Audit Log File Size

Description

The maximum size (in queries) of the Impala Daemon audit event log file before a new one is created.

Related Name

max_audit_event_log_file_size

Default Value

5000 line(s)

API Name

max_audit_event_log_file_size

Required

false

Impala Daemon Maximum Lineage Log File Size

Description

The maximum size (in entries) of the Impala daemon lineage log file before a new one is created.

Related Name

max_lineage_log_file_size

Default Value

5000 line(s)

API Name

max_lineage_log_file_size

Required

false

Impala Maximum Log Files

Description

The number of log files that are kept for each severity level before all older log files are removed. The number has to be greater than 1 to keep at least the current log file open. If set to 0, all log files are retained and log rotation is effectively disabled.

Related Name

max_log_files

Default Value

10

API Name

max_log_files

Required

false

Impala Daemon Max Log Size

Description

The maximum size, in megabytes, per log file for Impala Daemon logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Query Monitoring Timeout

Description

The timeout used by the Cloudera Manager Agent's query monitor when communicating with the Impala Daemon web server, specified in seconds.

Related Name

Default Value

15.0 second(s)

API Name

executing_queries_timeout_seconds

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Query Monitoring Failures Thresholds

Description

The health test thresholds for failures encountered when monitoring queries within a recent period specified by the impala_query_monitoring_failure_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

impala_query_monitoring_failure_thresholds

Required

false

Monitoring Period For Query Monitoring Failures

Description

The period to review when computing query monitoring failures.

Related Name

Default Value

5 minute(s)

API Name

impala_query_monitoring_failure_window

Required

false

Impala Daemon Query Collection Status Health Check

Description

Enables the health check that determines if query collection for the Impala Daemon is successful.

Related Name

Default Value

true

API Name

impala_query_monitoring_status_check_enabled

Required

false

Impala Daemon Connectivity Health Test

Description

Enables the health test that verifies the Impala Daemon is connected to the StateStore.

Related Name

Default Value

true

API Name

impalad_connectivity_health_enabled

Required

false

Impala Daemon Connectivity Tolerance at Startup

Description

The amount of time to wait for the Impala Daemon to fully start up and connect to the StateStore before enforcing the connectivity check.

Related Name

Default Value

3 minute(s)

API Name

impalad_connectivity_tolerance

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

impalad_fd_thresholds

Required

false

Impala Daemon Concurrent Client Connections Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of the number of concurrent client connections to Impala Daemon. Specified as a percentage of the maximum client connections parameter.

Related Name

Default Value

Warning: 80.0 %, Critical: 95.0 %

API Name

impalad_frontend_connections_thresholds

Required

false

Impala Daemon Host Health Test

Description

When computing the overall Impala Daemon health, consider the host's health.

Related Name

Default Value

true

API Name

impalad_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

impalad_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

impalad_pause_duration_window

Required

false

Impala Daemon Ready Status Health Check

Description

Enables the health check that determines if the Impala daemon is ready to process queries.

Related Name

Default Value

true

API Name

impalad_ready_status_check_enabled

Required

false

Impala Daemon Ready Status Startup Tolerance

Description

The amount of time at Impala Daemon startup allowed for the Impala Daemon to start accepting new queries for processing.

Related Name

Default Value

3 minute(s)

API Name

impalad_ready_status_check_startup_tolerance

Required

false

Impala Daemon Process Health Test

Description

Enables the health test that the Impala Daemon's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

impalad_scm_health_enabled

Required

false

Impala Daemon Scratch Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Impala Daemon Scratch Directories.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

impalad_scratch_directories_free_space_absolute_thresholds

Required

false

Impala Daemon Scratch Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Impala Daemon Scratch Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Impala Daemon Scratch Directories Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

impalad_scratch_directories_free_space_percentage_thresholds

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

impalad_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

impalad_web_metric_collection_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_resident_set_size_thresholds

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: Any, Critical: Any

API Name

process_swap_memory_thresholds

Required

false

Query Monitoring Full Sync Period

Description

The full sync period of the Impala query monitor in the Cloudera Manager Agent, specified in minutes. When a full sync is happening, all query profiles are sent over regardless of having been updated or not. If set to zero, a full sync is performed at each polling period.

Related Name

Default Value

3.0 minute(s)

API Name

query_monitoring_full_sync_period_minutes

Required

false

Query Monitoring Period

Description

The polling period of the Impala query monitor in the Cloudera Manager Agent, specified in seconds. If set to zero, query monitoring is disabled.

Related Name

Default Value

120.0 second(s)

API Name

query_monitoring_period_seconds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Impala Daemon Data Cache Per Directory Capacity

Description

Maximum amount of local disk space Impala will use per daemon in each of the configured directrories for caching of remote read data.

Related Name

Default Value

API Name

datacache_capacity

Required

false

Impala Daemon Data Cache Directories

Description

Directories Impala Daemon will use for caching of remote read data.

Related Name

Default Value

API Name

datacache_dirs

Required

false

Enable Local Data Cache

Description

Enable the local Impala Daemon data cache for caching of remote reads.

Related Name

Default Value

false

API Name

datacache_enabled

Required

false

Impala Daemon Default Query Options

Description

A list of key-value pairs of additional query options to pass to the Impala Daemon command line, separated by ','.

Related Name

default_query_options

Default Value

default_file_format=parquet default_transactional_type=insert_only

API Name

default_query_options

Required

false

Impala Graceful Shutdown Deadline

Description

Deadline (in seconds) for the graceful shutdown process of Impala Daemons. Once this deadline is reached, the daemon shuts down regardless of any running queries. A value of 0 means immediate shutdown.

Related Name

Default Value

5 minute(s)

API Name

impala_graceful_shutdown_deadline

Required

false

Impala Daemons Load Balancer

Description

Address of the load balancer used for Impala daemons. Should be specified in host:port format, where the port corresponds to the Beeswax protocol. If this is specified and Kerberos is enabled, Cloudera Manager adds a principal for 'impala/*load_balancer_host*@*realm*' to the keytab for all Impala daemons.

Related Name

Default Value

API Name

impalad_load_balancer

Required

false

Maximum Cached File Handles

Description

Maximum number of cached HDFS file handles. Caching HDFS file handles reduces the number of new file handles opened and thus reduces the load on the HDFS NameNode.. Each cached file handle consumes a small amount of memory on the Impala Daemon. If set to zero, the file handle caching is disabled.

Related Name

max_cached_file_handles

Default Value

20000

API Name

impalad_max_cached_file_handles

Required

false

Impala Daemon Specialization

Description

Configures Impala daemons to only execute queries or perform query coordination. When this setting is in use, daemons specializing in both tasks must exist.

Related Name

Default Value

NO_SPECIALIZATION

API Name

impalad_specialization

Required

false

Unused Cached File Handle Timeout

Description

Maximum time, in seconds, that an unused HDFS file handle will remain in the HDFS file handle cache. When the underlying file for a cached file handle is deleted, the disk space may not be freed until the cached file handle is removed from the cache. Specifying this timeout allows the disk space of deleted files to be freed in a predictable period of time. If set to zero, unused cached HDFS file handles do not time out.

Related Name

unused_file_handle_timeout_sec

Default Value

21600

API Name

impalad_unused_file_handle_timeout_sec

Required

false

Local UDF Library Dir

Description

User-defined function (UDF) libraries are copied from HDFS into this local directory.

Related Name

local_library_dir

Default Value

/var/lib/impala/udfs

API Name

local_library_dir

Required

false

Impala Daemon Scratch Directories

Description

Directories where Impala Daemon will write data such as spilling information to disk to free up memory. This can potentially be large amounts of data.

Related Name

scratch_dirs

Default Value

API Name

scratch_dirs

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Impala Daemon Backend Port

Description

Port on which thrift-based ImpalaInternalService is exported.

Related Name

be_port

Default Value

22000

API Name

be_port

Required

false

Impala Daemon Beeswax Port

Description

Port on which Beeswax client requests are served by Impala Daemons.

Related Name

beeswax_port

Default Value

21000

API Name

beeswax_port

Required

false

Impala Daemon HiveServer2 HTTP Port

Description

Port on which HiveServer2 client requests are served by Impala Daemons via HTTP.

Related Name

hs2_http_port

Default Value

28000

API Name

hs2_http_port

Required

false

Impala Daemon HiveServer2 Port

Description

Port on which HiveServer2 client requests are served by Impala Daemons via the thrift binary protocol.

Related Name

hs2_port

Default Value

21050

API Name

hs2_port

Required

false

Enable Impala Daemon Web Server

Description

Enable or disable the Impala Daemon web server. This web server contains useful information about Impala Daemon.

Related Name

enable_webserver

Default Value

true

API Name

impalad_enable_webserver

Required

false

Impala Daemon HTTP Server Port

Description

Port where Impala debug web server runs.

Related Name

webserver_port

Default Value

25000

API Name

impalad_webserver_port

Required

false

Impala Daemon KRPC Port

Description

Port on which KRPC-based ImpalaInternalService is exported.

Related Name

krpc_port

Default Value

27000

API Name

krpc_port

Required

false

Llama Callback Port

Description

Port where Llama notification callback should be started

Related Name

llama_callback_port

Default Value

0

API Name

llama_callback_port

Required

false

Second Statestore Host Name

Description

The hostname of the second statestore instance. Valid when statestore HA enabled.

Related Name

state_store_2_host

Default Value

API Name

state_store_2_host

Required

false

Second Statestore Port

Description

The port of statestore service running on the second statestore instance. Valid when statestore HA enabled.

Related Name

state_store_2_port

Default Value

24000

API Name

state_store_2_port

Required

false

Statestore Host Name

Description

The hostname of the statestore instance. When statestore HA is enabled, this stands for the first statestore instance.

Related Name

state_store_host

Default Value

API Name

state_store_host

Required

false

Statestore Port

Description

The port of statestore service running on the statestore instance. When statestore HA is enabled, this stands for the first statestore instance.

Related Name

state_store_port

Default Value

24000

API Name

state_store_port

Required

false

StateStoreSubscriber Service Port

Description

Port where StateStoreSubscriberService is running.

Related Name

state_store_subscriber_port

Default Value

23000

API Name

state_store_subscriber_port

Required

false

Resource Management

Java Heap Size of Impala Daemon in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Impala Daemon JVM Heap

Default Value

4 GiB

API Name

impalad_embedded_jvm_heapsize

Required

false

Idle Query Timeout

Description

The time that a query may be idle (i.e. no processing work is done and no updates are received from the client) before it is cancelled. If 0, idle queries are never expired.

Related Name

idle_query_timeout

Default Value

0 second(s)

API Name

impalad_idle_query_timeout

Required

false

Idle Session Timeout

Description

The time that a session may be idle before it is closed (and all running queries cancelled) by Impala. If 0, idle sessions are never expired.

Related Name

idle_session_timeout

Default Value

0 second(s)

API Name

impalad_idle_session_timeout

Required

false

Impala Daemon Memory Limit

Description

Memory limit for Impala Daemon, enforced by the daemon itself. This limit does not include memory consumed by the daemon's embedded JVM. The Impala Daemon uses up to this amount of memory for query processing, cached data, network buffers, background operations, etc. If exceeded, queries running on the Impala Daemon will be killed until the Impala Daemon is under the memory limit.

Related Name

mem_limit

Default Value

API Name

impalad_memory_limit

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Disk Spill Encryption

Description

Encrypt and verify the integrity of all data spilled to disk as part of a query. This feature is only supported for Impala 2.0 and higher and CDH 5.2 and higher (which includes Impala 2.0).

Related Name

disk_spill_encryption

Default Value

false

API Name

disk_spill_encryption

Required

false

LDAP Server CA Certificate

Description

The location on disk of the certificate, in .pem format, used to confirm the authenticity of the LDAP server certificate. This is the Certificate Authority (CA) certificate, and it was used to sign the LDAP server certificate. If not set, all certificates are trusted, which means that an attacker could potentially intercept otherwise encrypted usernames and passwords.

Related Name

ldap_ca_certificate

Default Value

API Name

impalad_ldap_ca_certificate

Required

false

JWKS Pull Timeout

Description

The time in seconds to wait for the JWKS to be downloaded from the specified URL before timing out.

Related Name

jwks_pulling_timeout_s

Default Value

10 second(s)

API Name

jwks_pulling_timeout_s

Required

false

JWKS Update Frequency

Description

The time in seconds to wait between re-downloading the JWKS from the specified URL.

Related Name

jwks_update_frequency_s

Default Value

10 second(s)

API Name

jwks_update_frequency_s

Required

false

JWKS URL

Description

URL where the JSON Web Key Set (JWKS) can be downloaded for JWT verification.

Related Name

jwks_url

Default Value

API Name

jwks_url

Required

false

Verify JWKS Server Certificate

Description

Specifies if the TLS certificate of the JWKS server is verified when retrieving the JWKS from the specified JWKS URL. This should only be set to false for development / testing.

Related Name

jwks_verify_server_certificate

Default Value

true

API Name

jwks_verify_server_certificate

Required

false

JWT Allow Without TLS

Description

Determines if JWT authentication is allowed without TLS being enabled on connections to the Impala daemon.

Related Name

jwt_allow_without_tls

Default Value

false

API Name

jwt_allow_without_tls

Required

false

Username JWT Custom Claim

Description

JWT claim that contains the username to use when authenticating with Impala.

Related Name

jwt_custom_claim_username

Default Value

API Name

jwt_custom_claim_username

Required

false

JWT Token Authentication

Description

Determines if JWT token authentication is enabled.

Related Name

jwt_token_auth

Default Value

false

API Name

jwt_token_auth

Required

false

JWT Validate Signature

Description

Determines if the signatures on incoming JWTs are validated against the JWKS.

Related Name

jwt_validate_signature

Default Value

true

API Name

jwt_validate_signature

Required

false

Impala Daemon Webserver TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Impala Daemon Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_certificate_file

Default Value

API Name

webserver_certificate_file

Required

false

Impala Daemon Web Server User Password

Description

Password for Impala Daemon webserver authentication.

Related Name

webserver_htpassword_password

Default Value

API Name

webserver_htpassword_password

Required

false

Impala Daemon Web Server Username

Description

Username for Impala Daemon webserver authentication.

Related Name

webserver_htpassword_user

Default Value

API Name

webserver_htpassword_user

Required

false

Impala Daemon Webserver TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Impala Daemon Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_private_key_file

Default Value

API Name

webserver_private_key_file

Required

false

Impala Daemon Webserver TLS/SSL Private Key Password

Description

The password for the private key in the Impala Daemon Webserver TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

webserver_private_key_password_cmd

Default Value

API Name

webserver_private_key_password_cmd

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Impala Daemon Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Audit Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_audit_event_log_dir

Required

true

Suppress Parameter Validation: Impala Daemon Backend Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Backend Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_be_port

Required

true

Suppress Parameter Validation: Impala Daemon Beeswax Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Beeswax Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_beeswax_port

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Impala Daemon Core Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Core Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_dump_dir

Required

true

Suppress Parameter Validation: Impala Daemon Data Cache Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Data Cache Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datacache_dirs

Required

true

Suppress Configuration Validator: Impala Daemon Default Memory Limit Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Default Memory Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_default_impalad_memory_limit_validator

Required

true

Suppress Parameter Validation: Impala Daemon Default Query Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Default Query Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_default_query_options

Required

true

Suppress Parameter Validation: Impala Daemon HiveServer2 HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon HiveServer2 HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_http_port

Required

true

Suppress Parameter Validation: Impala Daemon HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon HiveServer2 Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_port

Required

true

Suppress Configuration Validator: Impala Audit Enabled Validator

Description

Whether to suppress configuration warnings produced by the Impala Audit Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_audit_enabled_validator

Required

true

Suppress Parameter Validation: Impala Daemon HDFS Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon HDFS Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impala_hdfs_site_conf_safety_valve

Required

true

Suppress Parameter Validation: Impala Daemon Hive Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Hive Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impala_hive_conf_safety_valve

Required

true

Suppress Configuration Validator: Impala Lineage Enabled Validator

Description

Whether to suppress configuration warnings produced by the Impala Lineage Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_lineage_enabled_validator

Required

true

Suppress Parameter Validation: Impala Daemon Llama Site Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Llama Site Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impala_llama_site_conf_safety_valve

Required

true

Suppress Parameter Validation: Impala Daemon Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Command Line Argument Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_cmd_args_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon Command Line Arguments Safety Valve Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Command Line Arguments Safety Valve Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_cmd_args_safety_valve_validator

Required

true

Suppress Parameter Validation: Impala Daemon Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_core_site_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for Impala Daemon

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Impala Daemon parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_embedded_java_opts

Required

true

Suppress Parameter Validation: Impala Daemon Fair Scheduler Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Fair Scheduler Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_fair_scheduler_safety_valve

Required

true

Suppress Parameter Validation: Impala Daemon HBase Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon HBase Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_hbase_conf_safety_valve

Required

true

Suppress Parameter Validation: LDAP Server CA Certificate

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Server CA Certificate parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_ldap_ca_certificate

Required

true

Suppress Parameter Validation: Impala Daemons Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemons Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_load_balancer

Required

true

Suppress Parameter Validation: Impala Daemon Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_role_env_safety_valve

Required

true

Suppress Parameter Validation: Impala Daemon HTTP Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon HTTP Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_webserver_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: JWKS URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JWKS URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jwks_url

Required

true

Suppress Parameter Validation: Username JWT Custom Claim

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Username JWT Custom Claim parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jwt_custom_claim_username

Required

true

Suppress Parameter Validation: Impala Daemon KRPC Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon KRPC Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_krpc_port

Required

true

Suppress Parameter Validation: Impala Daemon Lineage Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Lineage Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_lineage_event_log_dir

Required

true

Suppress Parameter Validation: Llama Callback Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Llama Callback Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_llama_callback_port

Required

true

Suppress Parameter Validation: Local UDF Library Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Local UDF Library Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_local_library_dir

Required

true

Suppress Parameter Validation: Impala Daemon Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Impala Daemon Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Impala Daemon Breakpad Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Breakpad Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_minidump_path

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Impala Daemon Scratch Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Scratch Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_scratch_dirs

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Second Statestore Host Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Second Statestore Host Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_2_host

Required

true

Suppress Parameter Validation: Statestore Host Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore Host Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_host

Required

true

Suppress Parameter Validation: StateStoreSubscriber Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStoreSubscriber Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_subscriber_port

Required

true

Suppress Configuration Validator: Impala Daemon Unlimited Memory Limit Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Unlimited Memory Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_unlimited_impalad_memory_limit_validator

Required

true

Suppress Parameter Validation: Impala Daemon Webserver TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Webserver TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_certificate_file

Required

true

Suppress Parameter Validation: Impala Daemon Web Server User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Web Server User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_password

Required

true

Suppress Parameter Validation: Impala Daemon Web Server Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Web Server Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_user

Required

true

Suppress Parameter Validation: Impala Daemon Webserver TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Webserver TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_file

Required

true

Suppress Parameter Validation: Impala Daemon Webserver TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Daemon Webserver TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_password_cmd

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_audit_health

Required

true

Suppress Health Test: StateStore Connectivity

Description

Whether to suppress the results of the StateStore Connectivity heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_connectivity

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_file_descriptor

Required

true

Suppress Health Test: Impala Concurrent Client Connections

Description

Whether to suppress the results of the Impala Concurrent Client Connections heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_frontend_connections

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_log_directory_free_space

Required

true

Suppress Health Test: Resident Set Size

Description

Whether to suppress the results of the Resident Set Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_memory_rss_health

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_pause_duration

Required

true

Suppress Health Test: Query Monitoring Status Check

Description

Whether to suppress the results of the Query Monitoring Status Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_query_monitoring_status

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Impala Daemon Ready Check

Description

Whether to suppress the results of the Impala Daemon Ready Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_ready_status

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_scm_health

Required

true

Suppress Health Test: Impala Daemon Scratch Directories Free Space

Description

Whether to suppress the results of the Impala Daemon Scratch Directories Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_scratch_directories_free_space

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impalad_web_metric_collection

Required

true

Impala StateStore

Advanced

StateStore Core Dump Directory

Description

Directory where a StateStore core dump is placed.

Related Name

core_dump_dir

Default Value

/var/log/statestore

API Name

core_dump_dir

Required

false

Statestore Max Breakpad Dump Files

Description

Maximum number of Breakpad dump files stored by Statestore Role.

Related Name

max_minidumps

Default Value

9

API Name

max_minidumps

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Statestore Breakpad Dump Directory

Description

Directory for storing Statestore Breakpad dumps.

Related Name

minidump_path

Default Value

/var/log/impala-minidumps

API Name

minidump_path

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Statestore Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to StateStore command line flags.

Related Name

Default Value

API Name

statestore_cmd_args_safety_valve

Required

false

Impala StateStore Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STATESTORE_role_env_safety_valve

Required

false

Logs

StateStore Log Directory

Description

Directory where StateStore will place its log files.

Related Name

log_dir

Default Value

/var/log/statestore

API Name

log_dir

Required

false

Impala StateStore Logging Threshold

Description

The minimum log level for Impala StateStore logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

StateStore Verbose Log Level

Description

Verbose logging level for the GLog logger. These messages are always logged at 'INFO' log level, so this setting has no effect if Logging Threshold is set to 'WARN' or above.

Related Name

GLOG_v

Default Value

1

API Name

log_verbose_level

Required

false

StateStore Log Buffer Level

Description

Buffer log messages logged at this level or lower (-1 means don't buffer; 0 means buffer INFO only; 1 means buffer WARNING only, ...)

Related Name

logbuflevel

Default Value

0

API Name

logbuflevel

Required

false

StateStore Maximum Log Files

Description

The number of log files that are kept for each severity level before all older log files are removed. The number has to be greater than 1 to keep at least the current log file open. If set to 0, all log files are retained and log rotation is effectively disabled.

Related Name

max_log_files

Default Value

10

API Name

max_log_files

Required

false

Impala StateStore Max Log Size

Description

The maximum size, in megabytes, per log file for Impala StateStore logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Resident Set Size Thresholds

Description

The health test thresholds on the resident size of the process.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_resident_set_size_thresholds

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

statestore_fd_thresholds

Required

false

Impala StateStore Host Health Test

Description

When computing the overall Impala StateStore health, consider the host's health.

Related Name

Default Value

true

API Name

statestore_host_health_enabled

Required

false

Impala StateStore Process Health Test

Description

Enables the health test that the Impala StateStore's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

statestore_scm_health_enabled

Required

false

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Related Name

Default Value

5 minute(s)

API Name

statestore_startup_tolerance

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

statestore_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

statestore_web_metric_collection_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Catalog HA Preemption Wait Period

Description

Wait period before choosing the primary catalog server.

Related Name

catalogd_ha_preemption_wait_period_ms

Default Value

10 second(s)

API Name

statestore_catalogd_ha_preemption_wait_period_ms

Required

false

Enable StateStore Web Server

Description

Enable/Disable StateStore web server. This web server contains useful information about StateStore daemon.

Related Name

enable_webserver

Default Value

true

API Name

statestore_enable_webserver

Required

false

Force the Statestore active

Description

Set to true to force the statestored instance to take active role. Valid when statestore HA enabled.

Related Name

statestore_force_active

Default Value

false

API Name

statestore_force_active

Required

false

Statestore HA Preemption Wait Period

Description

The time after which statestored designates itself in active role if the statestore does not receive negotiation request from its peer statestore during start up.

Related Name

statestore_ha_preemption_wait_period_ms

Default Value

10 second(s)

API Name

statestore_ha_preemption_wait_period_ms

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

StateStore Worker Threads

Description

Number of worker threads for the thread manager underlying the StateStore Thrift server.

Related Name

state_store_num_server_worker_threads

Default Value

4

API Name

state_store_num_server_worker_threads

Required

false

Maximum StateStore Pending Tasks

Description

Maximum number of tasks allowed to be pending at the thread manager underlying the StateStore Thrift server (0 allows infinitely many pending tasks)

Related Name

state_store_pending_task_count_max

Default Value

0

API Name

state_store_pending_task_count_max

Required

false

Ports and Addresses

Statestore HA Port

Description

The port of Thrift service for communication between two statestore instances in HA pair. Valid when statestore HA enabled.

Related Name

state_store_ha_port

Default Value

24020

API Name

state_store_ha_port

Required

false

Peer Statestore Port

Description

The port of Thrift service of peer statestore instance for statestore HA. Valid when statestore HA enabled.

Related Name

state_store_peer_ha_port

Default Value

24020

API Name

state_store_peer_ha_port

Required

false

Peer Statestore Host Name

Description

The hostname of peer statesore instance in HA pair. Valid when statestore HA enabled.

Related Name

state_store_peer_host

Default Value

API Name

state_store_peer_host

Required

false

StateStore Service Port

Description

Port where StateStoreService is exported.

Related Name

state_store_port

Default Value

24000

API Name

state_store_port

Required

false

StateStore HTTP Server Port

Description

Port where StateStore debug web server runs.

Related Name

webserver_port

Default Value

25010

API Name

statestore_webserver_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

StateStore Webserver TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when StateStore Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_certificate_file

Default Value

API Name

webserver_certificate_file

Required

false

Statestore Web Server User Password

Description

Password for Statestore webserver authentication.

Related Name

webserver_htpassword_password

Default Value

API Name

webserver_htpassword_password

Required

false

Statestore Web Server Username

Description

Username for Statestore webserver authentication.

Related Name

webserver_htpassword_user

Default Value

API Name

webserver_htpassword_user

Required

false

StateStore Webserver TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when StateStore Webserver is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_private_key_file

Default Value

API Name

webserver_private_key_file

Required

false

StateStore Webserver TLS/SSL Private Key Password

Description

The password for the private key in the StateStore Webserver TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

webserver_private_key_password_cmd

Default Value

API Name

webserver_private_key_password_cmd

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: StateStore Core Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Core Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_dump_dir

Required

true

Suppress Parameter Validation: StateStore Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Statestore Breakpad Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore Breakpad Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_minidump_path

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Statestore HA Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore HA Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_ha_port

Required

true

Suppress Parameter Validation: Peer Statestore Host Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Peer Statestore Host Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_peer_host

Required

true

Suppress Parameter Validation: StateStore Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_port

Required

true

Suppress Parameter Validation: Statestore Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore Command Line Argument Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_cmd_args_safety_valve

Required

true

Suppress Parameter Validation: Impala StateStore Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala StateStore Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_role_env_safety_valve

Required

true

Suppress Parameter Validation: StateStore HTTP Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore HTTP Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_webserver_port

Required

true

Suppress Parameter Validation: StateStore Webserver TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Webserver TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_certificate_file

Required

true

Suppress Parameter Validation: Statestore Web Server User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore Web Server User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_password

Required

true

Suppress Parameter Validation: Statestore Web Server Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Statestore Web Server Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_user

Required

true

Suppress Parameter Validation: StateStore Webserver TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Webserver TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_file

Required

true

Suppress Parameter Validation: StateStore Webserver TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StateStore Webserver TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_password_cmd

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_log_directory_free_space

Required

true

Suppress Health Test: Resident Set Size

Description

Whether to suppress the results of the Resident Set Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_memory_rss_health

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_statestore_web_metric_collection

Required

true

Service-Wide

Admission Control

Enable Dynamic Resource Pools

Description

Use Dynamic Resource Pools to configure Impala admission control or RM for this Impala service. These features are only supported in Impala 1.3 or higher deployments.

Related Name

Default Value

true

API Name

admission_control_enabled

Required

false

Admission Control Queue Timeout

Description

Maximum amount of time (in milliseconds) that a request waits to be admitted before timing out. Must be a positive integer.

Related Name

queue_wait_timeout_ms

Default Value

1 minute(s)

API Name

admission_control_queue_timeout

Required

false

Single Pool Max Queued Queries

Description

Configures the maximum number of queued queries for admission control when using a single pool. -1 or 0 disables queuing, i.e. incoming requests are rejected if they can not be executed immediately. Ignored when Dynamic Resource Pools for Admission Control is enabled.

Related Name

default_pool_max_queued

Default Value

200

API Name

admission_control_single_pool_max_queued

Required

false

Single Pool Max Running Queries

Description

Configures the maximum number of concurrently running queries for admission control when using a single pool. -1 indicates no limit and 0 indicates all incoming requests will be rejected. Ignored when Dynamic Resource Pools for Admission Control is enabled.

Related Name

default_pool_max_requests

Default Value

200

API Name

admission_control_single_pool_max_requests

Required

false

Single Pool Mem Limit

Description

Configures the max memory of running queries for admission control when using a single pool. -1 or 0 indicates no limit. Ignored when Dynamic Resource Pools for Admission Control is enabled.

Related Name

default_pool_mem_limit

Default Value

-1 B

API Name

admission_control_single_pool_mem_limit

Required

false

Enable Impala Admission Control

Description

Use Impala Admission Control to throttle Impala requests. Unless 'Enable Dynamic Resource Pools' is enabled, Impala uses a single, default pool that is configured using the Single Pool configurations below. These features are only supported in Impala 1.3 or higher deployments.

Related Name

Default Value

true

API Name

all_admission_control_enabled

Required

false

Advanced

Impala Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

For advanced use only, a string to be inserted into atlas-application.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

application_properties_safety_valve

Required

false

Enable Core Dump

Description

Used to generate a core dump to get more information about an Impala crash. Unless otherwise configured systemwide using /proc/sys/kernel/core_pattern, the dump is generated in the 'current directory' of the Impala process (usually a subdirectory of the /var/run/cloudera-scm-agent/process directory). The core file can be very large.

Related Name

Default Value

false

API Name

enable_core_dump

Required

false

Maximum HBase Client Retries

Description

Maximum number of HBase client retries for Impala. Used as a maximum for all operations such as fetching of the root region from the root RegionServer, getting a cell's value, and starting a row update. Overrides configuration in the HBase service.

Related Name

hbase.client.retries.number

Default Value

3

API Name

hbase_client_retries_number

Required

false

HBase RPC Timeout

Description

Timeout in milliseconds for all HBase RPCs made by Impala. Overrides configuration in HBase service.

Related Name

hbase.rpc.timeout

Default Value

3 second(s)

API Name

hbase_rpc_timeout

Required

false

Impala Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be added (verbatim) to Impala Daemon command-line flags. Applies to all roles in this service. Key names should begin with a hyphen(-). For example: -log_filename=foo.log

Related Name

Default Value

API Name

impala_cmd_args_safety_valve

Required

false

Fair Scheduler Configuration Rules (Deployed)

Description

A list specifying the rules to run to determine which Fair Scheduler configuration to use. The value specified here is deployed to all hosts. This configuration has effect only on Impala versions 1.3 or greater.

Related Name

Default Value

[]

API Name

impala_schedule_rules

Required

false

Fair Scheduler Configuration Rules (Staged)

Description

A list specifying the rules to run to determine which Fair Scheduler configuration to use. Typically edited using the Rules configuration UI. This configuration only has effect on Impala versions 1.3 or greater.

Related Name

Default Value

API Name

impala_schedule_rules_draft

Required

false

Fair Scheduler Allocations (Deployed)

Description

JSON representation of all the configurations that the Fair Scheduler can take across all schedules. This configuration has effect only on Impala versions 1.3 or greater.

Related Name

Default Value

queues: [name: root, queues: [name: default, queues: [], schedulablePropertiesList: [scheduleName: default]], schedulablePropertiesList: [scheduleName: default]], users: []

API Name

impala_scheduled_allocations

Required

false

Fair Scheduler Allocations (Staged)

Description

JSON representation of all the configurations that the Fair Scheduler can take across all schedules. Typically edited using the Pools configuration UI. This configuration only has effect on Impala versions 1.3 or greater.

Related Name

Default Value

API Name

impala_scheduled_allocations_draft

Required

false

Impala Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

impala_service_env_safety_valve

Required

false

Impala Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml

Description

For advanced use only, a string to be inserted into sentry-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

impalad_sentry_safety_valve

Required

false

Use HDFS Rules to Map Kerberos Principals to Short Names

Description

If checked and Impala is using Kerberos, Impala will use the hadoop.security.auth_to_local rules from HDFS configuration. The relevant HDFS configuration is derived from Additional Rules to Map Kerberos Principals to Short Names.

Related Name

load_auth_to_local_rules

Default Value

false

API Name

load_hdfs_auth_to_local_rules

Required

false

Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.lineage.client.properties.

Related Name

Default Value

API Name

navigator_lineage_client_config_safety_valve

Required

false

Impala System Group (except Llama)

Description

The group that this Impala's processes should run as (except Llama, which has its own group).

Related Name

Default Value

impala

API Name

process_groupname

Required

true

Impala System User (except Llama)

Description

The user that this Impala's processes should run as (except Llama, which has its own user).

Related Name

Default Value

impala

API Name

process_username

Required

true

Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-audit.xml

Description

For advanced use only, a string to be inserted into ranger-impala-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-impala-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-security.xml

Description

For advanced use only, a string to be inserted into ranger-impala-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Use Debug Build

Description

Use debug build of Impala binaries when starting roles. Useful when performing diagnostic activities to get more information in the stacktrace or core dump.

Related Name

Default Value

false

API Name

use_debug_build

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for Impala events:

- userName: the user performing the action.
- ipAddress: the IP from where the request originated.
- operation: the Impala operation being performed.
- databaseName: the databaseName for the operation.
- tableName: the tableName for the operation.

Related Name

navigator.event.filter

Default Value

API Name

navigator_audit_event_filter

Required

false

Audit Queue Policy

Description

Action to take when the audit event queue is full. Drop the event or shutdown the affected process.

Related Name

navigator.batch.queue_policy

Default Value

DROP

API Name

navigator_audit_queue_policy

Required

false

Audit Event Tracker

Description

Configures the rules for event tracking and coalescing. This feature is used to define equivalency between different audit events. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the "tracked" events according to the rules defined here. Event trackers are defined in a JSON object like the following: { "timeToLive" : [integer], "fields" : [{ "type" : [string], "name" : [string] }] } Where:

- timeToLive: maximum amount of time an event will be tracked, in milliseconds. Must be provided. This defines how long, since it's first seen, an event will be tracked. A value of 0 disables tracking.
- fields: list of fields to compare when matching events against tracked events.

Each field has an evaluator type associated with it. The evaluator defines how the field data is to be compared. The following evaluators are available:

- value: uses the field value for comparison.
- userName: treats the field value as a userName, and ignores any host-specific data. This is useful for environment using Kerberos, so that only the principal name and realm are compared.

The following is the list of fields that can be used to compare Impala events:

- operation: the Impala operation being performed.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- databaseName: the database affected by the operation.
- tableName: the table affected by the operation.
- objectType: the type of object affected by the operation.
- privilege: the privilege associated with the operation.

Related Name

navigator_event_tracker

Default Value

API Name

navigator_event_tracker

Required

false

Enable Lineage Collection

Description

Enable collection of lineage from the service's roles.

Related Name

Default Value

true

API Name

navigator_lineage_enabled

Required

false

Monitoring

Admin Users Query List Visibility Settings

Description

Controls which queries admin users can see in the queries list view

Related Name

Default Value

ALL

API Name

admin_query_list_settings

Required

true

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Impala Catalog Server Monitoring Thresholds

Description

The health test thresholds of the overall Impala Catalog Server health. The check returns "Concerning" health if the percentage of "Healthy" Impala Catalog Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala Catalog Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 1.0 %

API Name

impala_catalogserver_healthy_thresholds

Required

false

Healthy Impala Daemon Monitoring Thresholds

Description

The health test thresholds of the overall Impala Daemon health. The check returns "Concerning" health if the percentage of "Healthy" Impala Daemons falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala Daemons falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

impala_impalads_healthy_thresholds

Required

false

Healthy Impala Llama ApplicationMaster Monitoring Thresholds

Description

The health test thresholds of the overall Impala Llama ApplicationMaster health. The check returns "Concerning" health if the percentage of "Healthy" Impala Llama ApplicationMasters falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala Llama ApplicationMasters falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

impala_llamas_healthy_thresholds

Required

false

Impala Query Aggregates

Description

Controls the aggregate metrics generated for Impala queries. The structure is a JSON list of the attributes to aggregate and the entities to aggregate to. For example, if the attributeName is 'hdfs_bytes_read' and the aggregationTargets is ['USER'] then the Service Monitor will create the metric 'impala_query_hdfs_bytes_read_rate' and, every ten minutes, will record the total hdfs bytes read for each user across all their Impala queries. By default it will also record the number of queries issues ('num_impala_queries_rate') for both users and pool. For a full list of the supported attributes see the Impala search page. Note that the valid aggregation targets are USER, YARN_POOL, and IMPALA (the service), and that these aggregate metrics can be viewed on both the reports and charts search pages.

Related Name

Default Value

[attributeName: hdfs_bytes_read, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: hdfs_bytes_written, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: thread_cpu_time, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: bytes_streamed, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: cm_cpu_milliseconds, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: query_duration, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: admission_wait, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: memory_accrual, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: thread_cpu_time, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER] , attributeName: memory_spilled, aggregationTargets: [USER, IMPALA_POOL_USER, IMPALA_POOL, IMPALA, CLUSTER]]

API Name

impala_query_aggregates

Required

false

Healthy Impala StateStore Monitoring Thresholds

Description

The health test thresholds of the overall Impala StateStore health. The check returns "Concerning" health if the percentage of "Healthy" Impala StateStores falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Impala StateStores falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 1.0 %

API Name

impala_statestore_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Non-Admin Users Query List Visibility Settings

Description

Controls which queries a non-admin user can see in the queries list view

Related Name

Default Value

ALL

API Name

user_query_list_settings

Required

true

Other

Atlas Service

Description

Name of the Atlas service that this Impala service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

Enable Profile Collection

Description

Enable collection of profile from the service's roles.

Related Name

Default Value

true

API Name

enable_telepub_profile_collection

Required

false

HBase Service

Description

Name of the HBase service that this Impala service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

false

HDFS Service

Description

Name of the HDFS service that this Impala service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Hive Service

Description

Name of the Hive service that this Impala service instance depends on

Related Name

Default Value

API Name

hive_service

Required

true

Kudu Service

Description

Name of the Kudu service that this Impala service instance depends on

Related Name

Default Value

API Name

kudu_service

Required

false

Enable Local Catalog

Description

With local catalog enabled, the coordinators pull metadata as needed from catalog and cache it locally.

Related Name

Default Value

true

API Name

local_catalog_enabled

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.hive.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin URL Auth Filesystem Schemes

Description

Set Ranger URL Auth Filesystem Schemes.

Related Name

ranger.plugin.hive.urlauth.filesystem.schemes

Default Value

hdfs:, file:, wasb:, adl:

API Name

ranger_plugin_urlauth_filesystem_schemes

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.hive.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Impala service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

YARN Service for Resource Management

Description

Name of YARN service to use for resource management integration between Impala and YARN. This service dependency and the existence of a Llama role is required for using said integration.

Related Name

Default Value

API Name

yarn_service

Required

false

ZooKeeper Service for Llama HA

Description

Name of the ZooKeeper service to use for leader election and fencing when Llama is configured for high availability. This service dependency is required when more than one Llama role is present.

Related Name

Default Value

API Name

zookeeper_service

Required

false

Performance

Enable HDFS Short-Circuit Read

Description

Enable HDFS short-circuit read. This allows a client colocated with the DataNode to read HDFS file blocks directly. This gives a performance boost to distributed clients that are aware of locality.

Related Name

dfs.client.read.shortcircuit

Default Value

true

API Name

dfs_client_read_shortcircuit

Required

false

StateStoreSubscriber Timeout

Description

Time in seconds before Impala Daemon or Catalog Server times out with the StateStore.

Related Name

statestore_subscriber_timeout_seconds

Default Value

30 second(s)

API Name

statestore_subscriber_timeout

Required

false

Security

Atlas Kafka Messages Spool Directory

Description

Spool directory for Atlas Kafka Messages.

Related Name

atlas.hook.spool.dir

Default Value

/var/log/impala/atlas-spool

API Name

atlas_message_spool_path

Required

false

Enable TLS/SSL for Impala

Description

Encrypt communication between clients and Impala using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

client_services_ssl_enabled

Default Value

false

API Name

client_services_ssl_enabled

Required

false

Enable LDAP Authentication

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

enable_ldap_auth

Default Value

false

API Name

enable_ldap_auth

Required

false

Enable LDAP TLS

Description

If true, attempts to establish a TLS (Transport Layer Security) connection with an LDAP server that was specified with ldap://. Not required when using an LDAP URL with prefix ldaps://, because that already specifies TLS. This option is also known as "Use StartTLS".

Related Name

ldap_tls

Default Value

false

API Name

enable_ldap_tls

Required

false

Enable Kerberos Authentication for HTTP Web-Consoles

Description

Enables Kerberos authentication for Hadoop HTTP web consoles for all roles of this service using the SPNEGO protocol. Note: This is effective only if Kerberos is enabled.

Related Name

Default Value

false

API Name

hadoop_secure_web_ui

Required

false

Proxy Group Configuration

Description

Specifies the set of authorized proxy groups (users who can impersonate other users belonging to the specified groups during authorization) and whom they are allowed to impersonate. Input is a semicolon-separated list of key=value pairs of authorized proxy users to the group(s) they can impersonate. These groups are specified as a comma separated list of groups, or '*' to indicate all groups. For example: joe=group1,group2;hue=*;admin=*. Only valid when Sentry is enabled.

Related Name

authorized_proxy_group_config

Default Value

API Name

impala_authorized_proxy_group_config

Required

false

Proxy User Configuration

Description

Specifies the set of authorized proxy users (users who can impersonate other users during authorization) and whom they are allowed to impersonate. Input is a semicolon-separated list of key=value pairs of authorized proxy users to the user(s) they can impersonate. These users are specified as a comma separated list of short usernames, or '*' to indicate all users. For example: joe=alice,bob;hue=*;admin=*. Only valid when Sentry is enabled.

Related Name

authorized_proxy_user_config

Default Value

hue=*;knox=*

API Name

impala_authorized_proxy_user_config

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

ldap_uri

Default Value

API Name

impala_ldap_uri

Required

false

impala TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that impala might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

impala_truststore_file

Required

false

impala TLS/SSL Trust Store Password

Description

The password for the impala TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

impala_truststore_password

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

impala

API Name

kerberos_princ_name

Required

true

Kerberos Re-init Interval

Description

Number of minutes between reestablishing our ticket with the Kerberos server.

Related Name

kerberos_reinit_interval

Default Value

1 hour(s)

API Name

kerberos_reinit_interval

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like "uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

ldap_baseDN

Default Value

API Name

ldap_baseDN

Required

false

LDAP Pattern

Description

When set, this parameter allows arbitrary mapping from usernames into a Distinguished Name (DN). The string specified must have a placeholder named "#UID" inside it, and that #UID is replaced with the username. For example, you could mimic the behavior of LDAP BaseDN by specifying "uid=#UID,ou=People,dc=cloudera,dc=com". When the username of "mike" comes in, it replaces the #UID and the result is "uid=mike,ou=People,dc=cloudera,dc=com". This option should be used when more control over the DN is needed. This parameter is mutually exclusive with LDAP Domain and LDAP BaseDN.

Related Name

ldap_bind_pattern

Default Value

API Name

ldap_bind_pattern

Required

false

Impala Client LDAP Password

Description

The password for connecting to Impala when using LDAP authentication. This is used by Cloudera Manager to execute Impala APIs like cancelling a query.

Related Name

ldap_cm_password

Default Value

API Name

ldap_cm_password

Required

false

Impala Client LDAP Username

Description

The username for connecting to Impala when using LDAP authentication. This is used by Cloudera Manager to execute Impala APIs like cancelling a query.

Related Name

ldap_cm_user

Default Value

API Name

ldap_cm_user

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

ldap_domain

Default Value

API Name

ldap_domain

Required

false

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/impala

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/impala/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/impala/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.hive.policy.cache.dir

Default Value

/var/lib/ranger/impala/policy-cache

API Name

ranger_policy_cache_dir

Required

false

The allowed set of OpenSSL ciphers

Description

A list of OpenSSL ciphers, optionally including other notation. See the output of 'man ciphers' for the full set of keywords and notation allowed in the arguments.

Related Name

ssl_cipher_list

Default Value

API Name

ssl_cipher_list

Required

false

Impala TLS/SSL CA Certificate

Description

The location on disk of the certificate, in PEM format, used to confirm the authenticity of SSL/TLS servers that the Impala daemons might connect to. Because the Impala daemons connect to each other, this should also include the CA certificate used to sign all the SSL/TLS Certificates. Without this parameter, SSL/TLS between Impala daemons will not be enabled.

Related Name

ssl_client_ca_certificate

Default Value

API Name

ssl_client_ca_certificate

Required

false

Impala TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Impala is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_private_key

Default Value

API Name

ssl_private_key

Required

false

Impala TLS/SSL Private Key Password

Description

The password for the private key in the Impala TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

ssl_private_key_password_cmd

Default Value

API Name

ssl_private_key_password

Required

false

Impala TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Impala is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_server_certificate

Default Value

API Name

ssl_server_certificate

Required

false

Suppressions

Suppress Configuration Validator: Impala Daemon Audit Log Directory

Description

Whether to suppress configuration warnings produced by the Impala Daemon Audit Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: Impala Daemon Backend Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon Backend Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_be_port

Required

true

Suppress Configuration Validator: Impala Daemon Beeswax Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon Beeswax Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_beeswax_port

Required

true

Suppress Configuration Validator: Catalog Server Service Port

Description

Whether to suppress configuration warnings produced by the Catalog Server Service Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalog_service_port

Required

true

Suppress Configuration Validator: Catalog Server Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Catalog Server Command Line Argument Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_cmd_args_safety_valve

Required

true

Suppress Configuration Validator: Impala Catalog Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the Impala Catalog Server Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_core_site_safety_valve

Required

true

Suppress Configuration Validator: Catalog Server HBase Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Catalog Server HBase Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hbase_conf_safety_valve

Required

true

Suppress Configuration Validator: Catalog Server HDFS Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Catalog Server HDFS Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hdfs_site_conf_safety_valve

Required

true

Suppress Configuration Validator: Catalog Server Hive Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Catalog Server Hive Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_hive_conf_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for Catalog Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Catalog Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogd_java_opts

Required

true

Suppress Configuration Validator: Impala Catalog Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Catalog Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: Catalog Server HTTP Server Port

Description

Whether to suppress configuration warnings produced by the Catalog Server HTTP Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_catalogserver_webserver_port

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Impala Daemon Core Dump Directory

Description

Whether to suppress configuration warnings produced by the Impala Daemon Core Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core_dump_dir

Required

true

Suppress Configuration Validator: Impala Daemon Data Cache Directories

Description

Whether to suppress configuration warnings produced by the Impala Daemon Data Cache Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datacache_dirs

Required

true

Suppress Configuration Validator: Impala Daemon Default Memory Limit Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Default Memory Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_default_impalad_memory_limit_validator

Required

true

Suppress Configuration Validator: Impala Daemon Default Query Options

Description

Whether to suppress configuration warnings produced by the Impala Daemon Default Query Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_default_query_options

Required

true

Suppress Configuration Validator: Impala Daemon HiveServer2 HTTP Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon HiveServer2 HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_http_port

Required

true

Suppress Configuration Validator: Impala Daemon HiveServer2 Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon HiveServer2 Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hs2_port

Required

true

Suppress Configuration Validator: Impala Audit Enabled Validator

Description

Whether to suppress configuration warnings produced by the Impala Audit Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_audit_enabled_validator

Required

true

Suppress Configuration Validator: Impala Daemon HDFS Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon HDFS Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_hdfs_site_conf_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon Hive Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Hive Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_hive_conf_safety_valve

Required

true

Suppress Configuration Validator: Impala Lineage Enabled Validator

Description

Whether to suppress configuration warnings produced by the Impala Lineage Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_lineage_enabled_validator

Required

true

Suppress Configuration Validator: Impala Daemon Llama Site Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Llama Site Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impala_llama_site_conf_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Command Line Argument Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_cmd_args_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon Command Line Arguments Safety Valve Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Command Line Arguments Safety Valve Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_cmd_args_safety_valve_validator

Required

true

Suppress Configuration Validator: Impala Daemon Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the Impala Daemon Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_core_site_safety_valve

Required

true

Suppress Configuration Validator: Java Configuration Options for Impala Daemon

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Impala Daemon configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_embedded_java_opts

Required

true

Suppress Configuration Validator: Impala Daemon Fair Scheduler Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Fair Scheduler Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_fair_scheduler_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon HBase Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon HBase Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_hbase_conf_safety_valve

Required

true

Suppress Configuration Validator: LDAP Server CA Certificate

Description

Whether to suppress configuration warnings produced by the LDAP Server CA Certificate configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_ldap_ca_certificate

Required

true

Suppress Configuration Validator: Impala Daemons Load Balancer

Description

Whether to suppress configuration warnings produced by the Impala Daemons Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_load_balancer

Required

true

Suppress Configuration Validator: Impala Daemon Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_role_env_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon HTTP Server Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon HTTP Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_impalad_webserver_port

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: JWKS URL

Description

Whether to suppress configuration warnings produced by the JWKS URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jwks_url

Required

true

Suppress Configuration Validator: Username JWT Custom Claim

Description

Whether to suppress configuration warnings produced by the Username JWT Custom Claim configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jwt_custom_claim_username

Required

true

Suppress Configuration Validator: Impala Daemon KRPC Port

Description

Whether to suppress configuration warnings produced by the Impala Daemon KRPC Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_krpc_port

Required

true

Suppress Configuration Validator: Impala Daemon Lineage Log Directory

Description

Whether to suppress configuration warnings produced by the Impala Daemon Lineage Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_lineage_event_log_dir

Required

true

Suppress Configuration Validator: Llama Callback Port

Description

Whether to suppress configuration warnings produced by the Llama Callback Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_llama_callback_port

Required

true

Suppress Configuration Validator: Local UDF Library Dir

Description

Whether to suppress configuration warnings produced by the Local UDF Library Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_local_library_dir

Required

true

Suppress Configuration Validator: Impala Daemon Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Impala Daemon Log Directory

Description

Whether to suppress configuration warnings produced by the Impala Daemon Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Impala Daemon Breakpad Dump Directory

Description

Whether to suppress configuration warnings produced by the Impala Daemon Breakpad Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_minidump_path

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Impala Daemon Scratch Directories

Description

Whether to suppress configuration warnings produced by the Impala Daemon Scratch Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_scratch_dirs

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Second Statestore Host Name

Description

Whether to suppress configuration warnings produced by the Second Statestore Host Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_2_host

Required

true

Suppress Configuration Validator: Statestore HA Port

Description

Whether to suppress configuration warnings produced by the Statestore HA Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_ha_port

Required

true

Suppress Configuration Validator: Statestore Host Name

Description

Whether to suppress configuration warnings produced by the Statestore Host Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_host

Required

true

Suppress Configuration Validator: Peer Statestore Host Name

Description

Whether to suppress configuration warnings produced by the Peer Statestore Host Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_peer_host

Required

true

Suppress Configuration Validator: StateStoreSubscriber Service Port

Description

Whether to suppress configuration warnings produced by the StateStoreSubscriber Service Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_state_store_subscriber_port

Required

true

Suppress Configuration Validator: Statestore Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Statestore Command Line Argument Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_cmd_args_safety_valve

Required

true

Suppress Configuration Validator: Impala StateStore Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Impala StateStore Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_role_env_safety_valve

Required

true

Suppress Configuration Validator: StateStore HTTP Server Port

Description

Whether to suppress configuration warnings produced by the StateStore HTTP Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_statestore_webserver_port

Required

true

Suppress Configuration Validator: Impala Daemon Unlimited Memory Limit Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Unlimited Memory Limit Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_unlimited_impalad_memory_limit_validator

Required

true

Suppress Configuration Validator: Impala Daemon Webserver TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Webserver TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_certificate_file

Required

true

Suppress Configuration Validator: Impala Daemon Web Server User Password

Description

Whether to suppress configuration warnings produced by the Impala Daemon Web Server User Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_password

Required

true

Suppress Configuration Validator: Impala Daemon Web Server Username

Description

Whether to suppress configuration warnings produced by the Impala Daemon Web Server Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_htpassword_user

Required

true

Suppress Configuration Validator: Impala Daemon Webserver TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Impala Daemon Webserver TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_file

Required

true

Suppress Configuration Validator: Impala Daemon Webserver TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Impala Daemon Webserver TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_private_key_password_cmd

Required

true

Suppress Parameter Validation: Impala Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Advanced Configuration Snippet (Safety Valve) for atlas-application.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_application_properties_safety_valve

Required

true

Suppress Parameter Validation: Atlas Kafka Messages Spool Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Kafka Messages Spool Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas_message_spool_path

Required

true

Suppress Configuration Validator: Impala Catalog Server Count Validator

Description

Whether to suppress configuration warnings produced by the Impala Catalog Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_catalogserver_count_validator

Required

true

Suppress Configuration Validator: Secure Web UI Validator

Description

Whether to suppress configuration warnings produced by the Secure Web UI Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_secure_web_ui

Required

true

Suppress Configuration Validator: Ranger Plugin Url Auth Validator for filesystem schemes

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Url Auth Validator for filesystem schemes configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hive_ranger_url_auth_validator

Required

true

Suppress Parameter Validation: Proxy Group Configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Group Configuration parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_authorized_proxy_group_config

Required

true

Suppress Parameter Validation: Proxy User Configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy User Configuration parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_authorized_proxy_user_config

Required

true

Suppress Configuration Validator: Bypass Hive Metastore Validator

Description

Whether to suppress configuration warnings produced by the Bypass Hive Metastore Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_bypass_hms_validator

Required

true

Suppress Parameter Validation: Impala Command Line Argument Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Command Line Argument Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_cmd_args_safety_valve

Required

true

Suppress Configuration Validator: Impala Command Line Arguments Safety Valve Validator

Description

Whether to suppress configuration warnings produced by the Impala Command Line Arguments Safety Valve Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_cmd_args_safety_valve_validator

Required

true

Suppress Configuration Validator: Impala Short-Circuit Read Validator

Description

Whether to suppress configuration warnings produced by the Impala Short-Circuit Read Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_dfs_client_read_shortcircuit_validator

Required

true

Suppress Configuration Validator: Enable HDFS Block Metadata API Configuration Validator

Description

Whether to suppress configuration warnings produced by the Enable HDFS Block Metadata API Configuration Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_hdfs_dfs_datanode_hdfs_blocks_metadata_enabled_set_validator

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_ldap_uri

Required

true

Suppress Configuration Validator: LDAP Configuration Validator

Description

Whether to suppress configuration warnings produced by the LDAP Configuration Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_ldap_validator

Required

true

Suppress Configuration Validator: Impala Llama Supported Validator

Description

Whether to suppress configuration warnings produced by the Impala Llama Supported Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_llama_supported_validator

Required

true

Suppress Parameter Validation: Impala Query Aggregates

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Query Aggregates parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_query_aggregates

Required

true

Suppress Parameter Validation: Impala Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_service_env_safety_valve

Required

true

Suppress Configuration Validator: Impala Specialization Validator

Description

Whether to suppress configuration warnings produced by the Impala Specialization Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impala_specialization_validator

Required

true

Suppress Parameter Validation: impala TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the impala TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_truststore_file

Required

true

Suppress Parameter Validation: impala TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the impala TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impala_truststore_password

Required

true

Suppress Configuration Validator: Impala Daemon Count Validator

Description

Whether to suppress configuration warnings produced by the Impala Daemon Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_impalad_count_validator

Required

true

Suppress Parameter Validation: Impala Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Advanced Configuration Snippet (Safety Valve) for sentry-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_impalad_sentry_safety_valve

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_basedn

Required

true

Suppress Parameter Validation: LDAP Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Pattern parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_bind_pattern

Required

true

Suppress Parameter Validation: Impala Client LDAP Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Client LDAP Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_cm_password

Required

true

Suppress Parameter Validation: Impala Client LDAP Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Client LDAP Username parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_cm_user

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_domain

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Audit Event Tracker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Tracker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_event_tracker

Required

true

Suppress Parameter Validation: Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Client Advanced Configuration Snippet (Safety Valve) for navigator.lineage.client.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_lineage_client_config_safety_valve

Required

true

Suppress Configuration Validator: CA Certificate File Validator

Description

Whether to suppress configuration warnings produced by the CA Certificate File Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_pem_ca_cert_recommended_for_ssl

Required

true

Suppress Parameter Validation: Impala System Group (except Llama)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala System Group (except Llama) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Impala System User (except Llama)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala System User (except Llama) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Plugin URL Auth Filesystem Schemes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin URL Auth Filesystem Schemes parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_urlauth_filesystem_schemes

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Service Advanced Configuration Snippet (Safety Valve) for ranger-impala-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Configuration Validator: Short-Circuit Read Enabled Validator

Description

Whether to suppress configuration warnings produced by the Short-Circuit Read Enabled Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_short_circuit_read_validator

Required

true

Suppress Configuration Validator: Short-Circuit Read Permissions Validator

Description

Whether to suppress configuration warnings produced by the Short-Circuit Read Permissions Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_short_circuit_reads_data_directory_permissions_validator

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: The allowed set of OpenSSL ciphers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the The allowed set of OpenSSL ciphers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_cipher_list

Required

true

Suppress Parameter Validation: Impala TLS/SSL CA Certificate

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala TLS/SSL CA Certificate parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_ca_certificate

Required

true

Suppress Parameter Validation: Impala TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_private_key

Required

true

Suppress Parameter Validation: Impala TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_private_key_password

Required

true

Suppress Parameter Validation: Impala TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_certificate

Required

true

Suppress Configuration Validator: Impala StateStore Count Validator

Description

Whether to suppress configuration warnings produced by the Impala StateStore Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_statestore_count_validator

Required

true

Suppress Health Test: Impala Catalog Server Health

Description

Whether to suppress the results of the Impala Catalog Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_impala_catalogserver_healthy

Required

true

Suppress Health Test: Impala Daemon Health

Description

Whether to suppress the results of the Impala Daemon Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_impala_impalads_healthy

Required

true

Suppress Health Test: Impala Llama ApplicationMaster Health

Description

Whether to suppress the results of the Impala Llama ApplicationMaster Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_impala_llamas_healthy

Required

true

Suppress Health Test: Impala StateStore Health

Description

Whether to suppress the results of the Impala StateStore Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_impala_statestore_healthy

Required

true

Java KeyStore KMS Properties in Cloudera Runtime 7.2.18

Role groups:

Key Management Server

Advanced

Key Management Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only. A string to be inserted into core-site.xml for this role only.

Related Name

Default Value

API Name

core-site.xml_role_safety_valve

Required

false

Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-acls.xml

Description

For advanced use only. A string to be inserted into kms-acls.xml for this role only.

Related Name

Default Value

API Name

kms-acls.xml_role_safety_valve

Required

false

Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-site.xml

Description

For advanced use only. A string to be inserted into kms-site.xml for this role only.

Related Name

Default Value

API Name

kms-site.xml_role_safety_valve

Required

false

Key Management Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KMS_role_env_safety_valve

Required

false

Key Management Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions

and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Key Management Server Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

For advanced use only. A string to be inserted into ssl-server.xml for this role only.

Related Name

Default Value

API Name

ssl-server.xml_role_safety_valve

Required

false

Logs

Key Management Server Log Directory

Description

The log directory for log files of the role Key Management Server.

Related Name

log.dir

Default Value

/var/log/hadoop-kms

API Name

log_dir

Required

false

Key Management Server Logging Threshold

Description

The minimum log level for Key Management Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Key Management Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Key Management Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Key Management Server Max Log Size

Description

The maximum size, in megabytes, per log file for Key Management Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kms_fd_thresholds

Required

false

Key Management Server Host Health Test

Description

When computing the overall Key Management Server health, consider the host's health.

Related Name

Default Value

true

API Name

kms_host_health_enabled

Required

false

Key Management Server Process Health Test

Description

Enables the health test that the Key Management Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kms_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Flume Proxy User Groups

Description

Allows the flume superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.flume.groups

Default Value

*

API Name

hadoop_kms_proxyuser_flume_groups

Required

false

Flume Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the flume user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.flume.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_flume_hosts

Required

false

HDFS Proxy User Groups

Description

Allows the hdfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hdfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_groups

Required

false

HDFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hdfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hdfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_hosts

Required

false

Hive Proxy User Groups

Description

Allows the hive superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hive.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hive_groups

Required

false

Hive Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hive user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hive.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hive_hosts

Required

false

HTTP Proxy User Groups

Description

Allows the HTTP superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.HTTP.groups

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_groups

Required

false

HTTP Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HTTP user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.HTTP.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_hosts

Required

false

HttpFS Proxy User Groups

Description

Allows the httpfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.httpfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_groups

Required

false

HttpFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the httpfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.httpfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_hosts

Required

false

Hue Proxy User Groups

Description

Allows the hue superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hue.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hue_groups

Required

false

Hue Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hue user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hue.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hue_hosts

Required

false

Mapred Proxy User Groups

Description

Allows the mapred superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.mapred.groups

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_groups

Required

false

Mapred Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the mapred user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.mapred.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_hosts

Required

false

Oozie Proxy User Groups

Description

Allows the oozie superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.oozie.groups

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_groups

Required

false

Oozie Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the oozie user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.oozie.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_hosts

Required

false

YARN Proxy User Groups

Description

Allows the yarn superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.yarn.groups

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_groups

Required

false

YARN Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the yarn user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.yarn.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_hosts

Required

false

JavaKeyStoreProvider Directory

Description

Directory of the keystore file kms.keystore used by JavaKeyStoreProvider that backs the KMS.

Related Name

hadoop.kms.key.provider.uri

Default Value

/var/lib/kms

API Name

hadoop_security_key_provider_dir

Required

true

KMS Accept Count

Description

The maximum queue length for incoming connection requests when all possible request processing threads are in use. Any requests received when the queue is full will be refused.This configuration is only supported in CDH 5.11 and up.

Related Name

hadoop.http.accept.queue.size

Default Value

500

API Name

kms_accept_count

Required

false

KMS Blacklist Users

Description

A comma-separated list of users (no spaces) for whom to disallow access to key material. These users can still fetch key metadata and create encrypted encryption keys, but are unable to do any other KMS operations. Typically, HDFS superusers will be specified here.

Related Name

kms_blacklist_users

Default Value

API Name

kms_blacklist_users

Required

false

KMS Heap Size

Description

Maximum heap size of the KMS.

Related Name

kms_heap_size

Default Value

1 GiB

API Name

kms_heap_size

Required

true

Additional Java Configuration Options for KMS

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

kms_java_opts

Default Value

API Name

kms_java_opts

Required

false

KMS Max Threads

Description

Maximum number of threads used to handle KMS requests.

Related Name

hadoop.http.max.threads

Default Value

250

API Name

kms_max_threads

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

KMS HTTP Port

Description

Port used by clients to interact with the KMS.

Related Name

hadoop.kms.http.port

Default Value

16000

API Name

kms_http_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Key Management Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Key Management Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.server.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Key Management Server TLS/SSL Trust Store Password

Description

The password for the Key Management Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.server.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Key Management Server

Description

Encrypt communication between clients and Key Management Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

hadoop.kms.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Key Management Server TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Key Management Server is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Key Management Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Key Management Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Key Management Server TLS/SSL Server Keystore File Password

Description

The password for the Key Management Server keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Key Management Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Flume Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flume Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_flume_groups

Required

true

Suppress Parameter Validation: Flume Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flume Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_flume_hosts

Required

true

Suppress Parameter Validation: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Parameter Validation: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Parameter Validation: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Parameter Validation: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Parameter Validation: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Parameter Validation: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Parameter Validation: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Parameter Validation: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Parameter Validation: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Parameter Validation: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Parameter Validation: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Parameter Validation: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Parameter Validation: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Parameter Validation: JavaKeyStoreProvider Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JavaKeyStoreProvider Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_key_provider_dir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-acls.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-acls.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms-acls.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: KMS Blacklist Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the KMS Blacklist Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms_blacklist_users

Required

true

Suppress Parameter Validation: KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the KMS HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms_http_port

Required

true

Suppress Parameter Validation: Additional Java Configuration Options for KMS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Java Configuration Options for KMS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms_java_opts

Required

true

Suppress Parameter Validation: Key Management Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms_role_env_safety_valve

Required

true

Suppress Parameter Validation: Key Management Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Key Management Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Key Management Server Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server Advanced Configuration Snippet (Safety Valve) for ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Key Management Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Key Management Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Key Management Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Key Management Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Key Management Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Management Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kms_kms_unexpected_exits

Required

true

Service-Wide

Advanced

Java KeyStore KMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

KMS_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Authentication Type

Description

Authentication type for the KMS. Can either be "simple" or "kerberos".

Related Name

hadoop.kms.authentication.type

Default Value

simple

API Name

hadoop_kms_authentication_type

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Key Management Server Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the Key Management Server Advanced Configuration Snippet (Safety Valve) for core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Flume Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Flume Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_flume_groups

Required

true

Suppress Configuration Validator: Flume Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Flume Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_flume_hosts

Required

true

Suppress Configuration Validator: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Configuration Validator: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Configuration Validator: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Configuration Validator: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Configuration Validator: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Configuration Validator: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Configuration Validator: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Configuration Validator: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Configuration Validator: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Configuration Validator: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Configuration Validator: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Configuration Validator: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Configuration Validator: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Configuration Validator: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Configuration Validator: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Configuration Validator: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Configuration Validator: JavaKeyStoreProvider Directory

Description

Whether to suppress configuration warnings produced by the JavaKeyStoreProvider Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_key_provider_dir

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-acls.xml

Description

Whether to suppress configuration warnings produced by the Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-acls.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms-acls.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-site.xml

Description

Whether to suppress configuration warnings produced by the Key Management Server Advanced Configuration Snippet (Safety Valve) for kms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: KMS Blacklist Users

Description

Whether to suppress configuration warnings produced by the KMS Blacklist Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms_blacklist_users

Required

true

Suppress Configuration Validator: KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the KMS HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms_http_port

Required

true

Suppress Configuration Validator: Additional Java Configuration Options for KMS

Description

Whether to suppress configuration warnings produced by the Additional Java Configuration Options for KMS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms_java_opts

Required

true

Suppress Configuration Validator: Key Management Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Key Management Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms_role_env_safety_valve

Required

true

Suppress Configuration Validator: Key Management Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Key Management Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Key Management Server Log Directory

Description

Whether to suppress configuration warnings produced by the Key Management Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Key Management Server Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

Whether to suppress configuration warnings produced by the Key Management Server Advanced Configuration Snippet (Safety Valve) for ssl-server.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl-server.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Key Management Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Key Management Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Key Management Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Key Management Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Key Management Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Key Management Server TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Key Management Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Key Management Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Key Management Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Key Management Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Key Management Server Count Validator

Description

Whether to suppress configuration warnings produced by the Key Management Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kms_count_validator

Required

true

Suppress Parameter Validation: Java KeyStore KMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java KeyStore KMS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kms_service_env_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Kafka Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/kafka

API Name

client_config_root_dir

Required

true

Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-client.conf

Description

For advanced use only, a string to be inserted into the client configuration for kafka-conf/kafka-client.conf.

Related Name

Default Value

API Name

kafka-conf/kafka-client.conf_client_config_safety_valve

Required

false

Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-ranger-repo.properties

Description

For advanced use only, a string to be inserted into the client configuration for kafka-conf/kafka-ranger-repo.properties.

Related Name

Default Value

API Name

kafka-conf/kafka-ranger-repo.properties_client_config_safety_valve

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-client.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-client.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-conf/kafka-client.conf_client_config_safety_valve

Required

true

Suppress Parameter Validation: Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-ranger-repo.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-ranger-repo.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-conf/kafka-ranger-repo.properties_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Kafka Broker

Advanced

Kafka Broker Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

For advanced use only. A string to be inserted into atlas-application.properties for this role only.

Related Name

Default Value

API Name

atlas-application.properties_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka-monitoring.properties

Description

For advanced use only. A string to be inserted into kafka-monitoring.properties for this role only.

Related Name

Default Value

API Name

kafka-monitoring.properties_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka.properties

Description

For advanced use only. A string to be inserted into kafka.properties for this role only.

Related Name

Default Value

API Name

kafka.properties_role_safety_valve

Required

false

Kafka Broker Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KAFKA_BROKER_role_env_safety_valve

Required

false

Kafka Broker Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-audit.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-audit.xml_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-security.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-security.xml_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

For advanced use only. A string to be inserted into ssl.properties for this role only.

Related Name

Default Value

API Name

ssl.properties_role_safety_valve

Required

false

Kafka Broker Advanced Configuration Snippet (Safety Valve) for zookeeper-ssl.properties

Description

For advanced use only. A string to be inserted into zookeeper-ssl.properties for this role only.

Related Name

Default Value

API Name

zookeeper-ssl.properties_role_safety_valve

Required

false

Logs

Kafka Broker Log Directory

Description

The log directory for log files of the role Kafka Broker.

Related Name

kafka.log4j.dir

Default Value

/var/log/kafka

API Name

log_dir

Required

false

Kafka Broker Logging Threshold

Description

The minimum log level for Kafka Broker logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Kafka Broker Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Kafka Broker logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Kafka Broker Max Log Size

Description

The maximum size, in megabytes, per log file for Kafka Broker logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Enable Lagging Replicas Test

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KAFKA-KAFKA_BROKER-7.2.0-LAGGING_REPLICAS_test_enable

Required

false

Enable Network Processor Capacity Test

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KAFKA-KAFKA_BROKER-7.2.0-NETWORK_PROCESSOR_CAPACITY_test_enable

Required

false

Enable Offline Directory Test

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KAFKA-KAFKA_BROKER-7.2.0-OFFLINE_DIRECTORIES_test_enable

Required

false

Enable Offline Partitions Test

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KAFKA-KAFKA_BROKER-7.2.0-OFFLINE_PARTITIONS_test_enable

Required

false

Enable Request Handler Capacity Test

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KAFKA-KAFKA_BROKER-7.2.0-REQUEST_HANDLER_CAPACITY_test_enable

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kafka_broker_fd_thresholds

Required

false

Kafka Broker Host Health Test

Description

When computing the overall Kafka Broker health, consider the host's health.

Related Name

Default Value

true

API Name

kafka_broker_host_health_enabled

Required

false

Kafka Broker Process Health Test

Description

Enables the health test that the Kafka Broker's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kafka_broker_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Advertised Host

Description

If set, this is the hostname given out to producers, consumers, and other brokers to use in establishing connections. Never set this property at the group level; it should always be overriden on instance level.

Related Name

advertised.host.name

Default Value

API Name

advertised.host.name

Required

false

Enable Auditing to Atlas

Description

When enabled, Kafka will audit Kafka Topics, Producers and Consumers to Atlas

Related Name

atlas.audit.enabled

Default Value

false

API Name

atlas.audit.enabled

Required

false

Authenticate Zookeeper Connection

Description

Enables authentication of SASL connections with zookeeper, if Kerberos authentication is enabled. It also allows a broker to set SASL ACL on zookeeper nodes, which locks these nodes down so that only a Kafka broker can modify it.

Related Name

authenticate.zookeeper.connection

Default Value

true

API Name

authenticate.zookeeper.connection

Required

false

Broker ID

Description

ID uniquely identifying each broker. Never set this property at the group level; it should always be overridden on instance level.

Related Name

broker.id

Default Value

API Name

broker.id

Required

false

Additional Broker Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags are passed here.

Related Name

broker_java_opts

Default Value

-server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -XX:G1HeapRegionSize=16M -XX:MinMetaspaceFreeRatio=50 -XX:MaxMetaspaceFreeRatio=80 -XX:+DisableExplicitGC -Djava.awt.headless=true -Djava.net.preferIPv4Stack=true -Dcom.sun.management.jmxremote.host=127.0.0.1 -Dcom.sun.management.jmxremote.local.only=true -Djava.rmi.server.hostname=127.0.0.1

API Name

broker_java_opts

Required

false

Java Heap Size of Broker

Description

Maximum size for the Java process heap memory. Passed to Java -Xmx. Measured in megabytes. Kafka does not generally require setting large heap sizes. It is better to let the file system cache utilize the available memory.

Related Name

broker_max_heap_size

Default Value

1 GiB

API Name

broker_max_heap_size

Required

false

Kafka Broker Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Enable Rack Awareness

Description

Enable rack awareness. If it is enabled, broker.rack property is set for each broker according to rack settings for the hosts in CM.

Related Name

enable.rack.awareness

Default Value

false

API Name

enable.rack.awareness

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

2 minute(s)

API Name

graceful_stop_timeout

Required

false

Enable Authenticated Communication with the JMX Agent

Description

Enables Authenticated Communication with the JMX Agent.

Related Name

jmx.auth.enabled

Default Value

false

API Name

jmx.auth.enabled

Required

false

Name of User with Read-Write Access to the JMX Agent

Description

Specifies the name of the user that has read-write privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.control.user

Default Value

controlRole

API Name

jmx.control.user

Required

false

Password of user with read-write access to the JMX agent

Description

Specifies the password of the user that has read-write privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.control.user.passwd

Default Value

API Name

jmx.control.user.passwd

Required

false

Name of User with read-only access to the JMX Agent

Description

Specifies the name of the user that has read-only privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.monitor.user

Default Value

monitorRole

API Name

jmx.monitor.user

Required

false

Password of User with read-only Access to the JMX agent

Description

Specifies the password of the user that has read-only privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.monitor.user.passwd

Default Value

API Name

jmx.monitor.user.passwd

Required

false

Enable TLS client authentication for JMX port

Description

If enabled, a valid client certificate must be presented by the JMX client in order to connect to the JMX port. Ensure that the trusted CA certificates are present in either the Kafka JMX TLS/SSL Server Trust Store file or the global trust store.

Related Name

jmx.ssl.client.auth.enabled

Default Value

false

API Name

jmx.ssl.client.auth.enabled

Required

false

Enable TLS/SSL for Kafka JMX

Description

Encrypt communication between clients and Kafka JMX using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

jmx.ssl.enabled

Default Value

false

API Name

jmx.ssl.enabled

Required

false

Enable HTTP Metric Report Basic Authentication

Description

Enable Basic Authentication for Kafka Metric HTTP Endpoint.

Related Name

kafka.http.metrics.authentication.enabled

Default Value

false

API Name

kafka.http.metrics.authentication.enabled

Required

false

HTTP Metric Report Host

Description

The host that the HTTP metric reporter binds to.

Related Name

kafka.http.metrics.host

Default Value

0.0.0.0

API Name

kafka.http.metrics.host

Required

false

HTTP Metric Report Password

Description

The password used for Basic Authentication.

Related Name

kafka.http.metrics.password

Default Value

API Name

kafka.http.metrics.password

Required

false

SSL Encryption For HTTP Metric Reporter

Description

Enable SSL Encryption for HTTP Metrics Endpoint. IMPORTANT: SSL encryption will be enabled if ssl_enabled config is enabled as well!

Related Name

kafka.http.metrics.ssl.enabled

Default Value

false

API Name

kafka.http.metrics.ssl.enabled

Required

false

HTTP Metric Report User

Description

The username used for Basic Authentication.

Related Name

kafka.http.metrics.user

Default Value

API Name

kafka.http.metrics.user

Required

false

Data Directories

Description

A list of one or more directories in which Kafka data is stored.. Each new partition created is placed in the directory that currently has the least amount of partitions.. Each directory should be on its own separate drive.

Related Name

log.dirs

Default Value

/var/local/kafka/data

API Name

log.dirs

Required

true

Data Retention Size

Description

The amount of data to retain in the log for each topic-partition. This is the limit per partition. Multiply it by the number of partitions to get the total amount of data retained for the topic. This property can take -1 as a value, which is interpreted as unlimited. If both log.retention.ms and log.retention.bytes are set, a segment is deleted when either limit is exceeded.

Related Name

log.retention.bytes

Default Value

-1 B

API Name

log.retention.bytes

Required

false

Data Retention Check Interval

Description

The frequency, in milliseconds, that the log cleaner checks whether any log segment is eligible for deletion, per retention policies.

Related Name

log.retention.check.interval.ms

Default Value

5 minute(s)

API Name

log.retention.check.interval.ms

Required

false

Data Retention Time

Description

The maximum time before a new log segment is rolled out. If both log.retention.ms and log.retention.bytes are set, a segment is deleted when either limit is exceeded. This property can take -1 as a value, which is interpreted as unlimited.

Related Name

log.retention.ms

Default Value

7 day(s)

API Name

log.retention.ms

Required

true

Data Log Roll Time

Description

The maximum time before a new log segment is rolled out.

Related Name

log.roll.ms

Default Value

API Name

log.roll.ms

Required

false

Segment File Size

Description

The log for a topic partition is stored as a directory of segment files. This setting controls the size to which a segment file can grow before a new segment is rolled over in the log. This value has to be larger than message.max.bytes.

Related Name

log.segment.bytes

Default Value

1 GiB

API Name

log.segment.bytes

Required

false

Maximum Connections per IP Address

Description

Maximum number of connections allowed from each IP address.

Related Name

max.connections.per.ip

Default Value

API Name

max.connections.per.ip

Required

false

Number of I/O Threads

Description

The number of I/O threads that the server uses for executing requests. You should have at least as many threads as you have disks.

Related Name

num.io.threads

Default Value

8

API Name

num.io.threads

Required

false

Number of Network Threads

Description

Number of threads that the server uses to handle incoming requests and outgoing responses.

Related Name

num.network.threads

Default Value

8

API Name

num.network.threads

Required

false

Number of Recovery Threads per data directory

Description

Number of threads per data directory that the server uses for log recovery during startup and log flushing during shutdown. Increasing this value may improve broker startup performance if you have a high number of segments. The total number of recovery threads (number of threads per data dir * number of data dirs) should not exceed the number of CPU cores. The default value is 1.

Related Name

num.recovery.threads.per.data.dir

Default Value

1

API Name

num.recovery.threads.per.data.dir

Required

false

Number of Alter Log Dir Threads

Description

Number of threads that the server uses to move data between log directories. The default value of this property is the same as the number of log directories.

Related Name

num.replica.alter.log.dirs.threads

Default Value

API Name

num.replica.alter.log.dirs.threads

Required

false

Ranger Kafka Plugin Conf Path

Description

Staging directory for Ranger Kafka Plugin Configuration. This should generally not be changed.

Related Name

ranger_kafka_plugin_conf_path

Default Value

/etc/ranger/kafka-plugin

API Name

ranger_kafka_plugin_conf_path

Required

true

Ranger Kafka Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/kafka/audit/hdfs/spool

API Name

ranger_kafka_plugin_hdfs_audit_spool_directory

Required

true

Ranger Kafka Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.kafka.policy.cache.dir

Default Value

/var/lib/ranger/kafka/policy-cache

API Name

ranger_kafka_plugin_policy_cache_directory

Required

true

Ranger Kafka Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/kafka/audit/solr/spool

API Name

ranger_kafka_plugin_solr_audit_spool_directory

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.kafka.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.kafka.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Inter Broker Protocol

Description

Protocol to be used for inter-broker communication. INFERRED uses the same protocol that is configured for external clients.

Related Name

security.inter.broker.protocol

Default Value

INFERRED

API Name

security.inter.broker.protocol

Required

false

Socket receive buffer size.

Description

The SO_RCVBUF buffer of the socket server sockets. If the value is -1, the OS default will be used.

Related Name

socket.receive.buffer.bytes

Default Value

100 KiB

API Name

socket.receive.buffer.bytes

Required

false

Socket receive buffer size.

Description

The maximum number of bytes in a socket request

Related Name

socket.request.max.bytes

Default Value

100 MiB

API Name

socket.request.max.bytes

Required

false

Socket send buffer size.

Description

The SO_SNDBUF buffer of the socket server sockets. If the value is -1, the OS default will be used.

Related Name

socket.send.buffer.bytes

Default Value

100 KiB

API Name

socket.send.buffer.bytes

Required

false

SSL Client Authentication

Description

Client authentication mode for SSL connections. This configuration has three valid values, "required", "requested" and "none". If set to "required", client authentication is required. If set to "requested", client authentication is requested and clients without certificates can still connect. If set to "none", which is the default value, no client authentication is required.

Related Name

ssl.client.auth

Default Value

none

API Name

ssl.client.auth

Required

false

Enable Zookeeper ACL

Description

Enables brokers to set SASL ACL on zookeeper nodes if authenticate.zookeeper.connection is enabled.

Related Name

zookeeper.set.acl

Default Value

true

API Name

zookeeper.set.acl

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Advertised Port

Description

The port to give out to producers, consumers, and other brokers to use in establishing connections. This only needs to be set if this port is different from the port the server should bind to.

Related Name

advertised.port

Default Value

API Name

advertised.port

Required

false

JMX Port

Description

Port for JMX.

Related Name

jmx_port

Default Value

9393

API Name

jmx_port

Required

false

HTTP Metric Report Port

Description

The port that the HTTP metric reporter listens on.

Related Name

kafka.http.metrics.port

Default Value

24042

API Name

kafka.http.metrics.port

Required

false

TCP Port

Description

Kafka broker port.

Related Name

port

Default Value

9092

API Name

port

Required

false

TLS/SSL Port

Description

Kafka broker secure port.

Related Name

ssl_port

Default Value

9093

API Name

ssl_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Kafka Broker TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Kafka Broker might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Kafka Broker TLS/SSL Trust Store Password

Description

The password for the Kafka Broker TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password.generator

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Kafka Broker

Description

Encrypt communication between clients and Kafka Broker using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Kafka Broker TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Kafka Broker is acting as a TLS/SSL server.

Related Name

ssl.key.password.generator

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Kafka Broker TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Kafka Broker is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Kafka Broker TLS/SSL Server Keystore File Password

Description

The password for the Kafka Broker keystore file.

Related Name

ssl.keystore.password.generator

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Advertised Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advertised Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_advertised.host.name

Required

true

Suppress Parameter Validation: Advertised Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advertised Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_advertised.port

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for atlas-application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas-application.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Broker ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Broker ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_broker.id

Required

true

Suppress Parameter Validation: Additional Broker Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Broker Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_broker_java_opts

Required

true

Suppress Parameter Validation: Java Heap Size of Broker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of Broker parameter.

Related Name

Default Value

false

API Name

role_config_suppression_broker_max_heap_size

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Name of User with Read-Write Access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with Read-Write Access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user

Required

true

Suppress Parameter Validation: Password of user with read-write access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of user with read-write access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user.passwd

Required

true

Suppress Parameter Validation: Name of User with read-only access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with read-only access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user

Required

true

Suppress Parameter Validation: Password of User with read-only Access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of User with read-only Access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user.passwd

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: JMX Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_port

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka-monitoring.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka-monitoring.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-monitoring.properties_role_safety_valve

Required

true

Suppress Parameter Validation: HTTP Metric Report Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Metric Report Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.host

Required

true

Suppress Parameter Validation: HTTP Metric Report Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Metric Report Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.password

Required

true

Suppress Parameter Validation: HTTP Metric Report Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Metric Report Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.port

Required

true

Suppress Parameter Validation: HTTP Metric Report User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Metric Report User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.user

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka Broker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_broker_role_env_safety_valve

Required

true

Suppress Parameter Validation: Data Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log.dirs

Required

true

Suppress Parameter Validation: Segment File Size

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Segment File Size parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log.segment.bytes

Required

true

Suppress Parameter Validation: Kafka Broker Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Kafka Broker Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Number of I/O Threads

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of I/O Threads parameter.

Related Name

Default Value

false

API Name

role_config_suppression_num.io.threads

Required

true

Suppress Parameter Validation: Number of Network Threads

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Network Threads parameter.

Related Name

Default Value

false

API Name

role_config_suppression_num.network.threads

Required

true

Suppress Parameter Validation: Number of Recovery Threads per data directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Recovery Threads per data directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_num.recovery.threads.per.data.dir

Required

true

Suppress Parameter Validation: Number of Alter Log Dir Threads

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Alter Log Dir Threads parameter.

Related Name

Default Value

false

API Name

role_config_suppression_num.replica.alter.log.dirs.threads

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: TCP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TCP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_port

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Kafka Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kafka Plugin Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_conf_path

Required

true

Suppress Parameter Validation: Ranger Kafka Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kafka Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Kafka Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kafka Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Kafka Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kafka Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ssl.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka Broker TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Kafka Broker TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: TLS/SSL Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_port

Required

true

Suppress Parameter Validation: Kafka Broker TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Kafka Broker TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Kafka Broker TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kafka Broker Advanced Configuration Snippet (Safety Valve) for zookeeper-ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Broker Advanced Configuration Snippet (Safety Valve) for zookeeper-ssl.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper-ssl.properties_role_safety_valve

Required

true

Suppress Health Test: Lagging Replicas Test

Description

Whether to suppress the results of the Lagging Replicas Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka-kafka_broker-7.2.0-lagging_replicas

Required

true

Suppress Health Test: Network Processor Capacity Test

Description

Whether to suppress the results of the Network Processor Capacity Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka-kafka_broker-7.2.0-network_processor_capacity

Required

true

Suppress Health Test: Offline Directory Test

Description

Whether to suppress the results of the Offline Directory Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka-kafka_broker-7.2.0-offline_directories

Required

true

Suppress Health Test: Offline Partitions Test

Description

Whether to suppress the results of the Offline Partitions Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka-kafka_broker-7.2.0-offline_partitions

Required

true

Suppress Health Test: Request Handler Capacity Test

Description

Whether to suppress the results of the Request Handler Capacity Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka-kafka_broker-7.2.0-request_handler_capacity

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_broker_unexpected_exits

Required

true

Kafka Connect

Advanced

Kafka Connect Advanced Configuration Snippet (Safety Valve) for connect-distributed.properties

Description

For advanced use only. A string to be inserted into connect-distributed.properties for this role only.

Related Name

Default Value

API Name

connect-distributed.properties_role_safety_valve

Required

false

Kafka Connect Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KAFKA_CONNECT_role_env_safety_valve

Required

false

Kafka Connect Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Kafka Connect Log Directory

Description

The log directory for log files of the role Kafka Connect.

Related Name

kafka_connect.log4j.dir

Default Value

/var/log/kafka

API Name

log_dir

Required

false

Kafka Connect Logging Threshold

Description

The minimum log level for Kafka Connect logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Kafka Connect Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Kafka Connect logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Kafka Connect Max Log Size

Description

The maximum size, in megabytes, per log file for Kafka Connect logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kafka_connect_fd_thresholds

Required

false

Kafka Connect Host Health Test

Description

When computing the overall Kafka Connect health, consider the host's health.

Related Name

Default Value

true

API Name

kafka_connect_host_health_enabled

Required

false

Kafka Connect Process Health Test

Description

Enables the health test that the Kafka Connect's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kafka_connect_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Bootstrap Servers

Description

A comma-separated list of IP:port or hostname:port pairs of the brokers that Kafka Connect should connect to. The brokers you specify here must be brokers that are running in the same cluster that Kafka Connect is deployed in. Cloudera recommends that you specify multiple brokers for high availability.

Related Name

bootstrap.servers

Default Value

API Name

bootstrap.servers

Required

true

Configuration Storage Topic Replication Factor

Description

Replication factor used when creating the configuration storage topic.

Related Name

config.storage.replication.factor

Default Value

1

API Name

config.storage.replication.factor

Required

true

Configuration Storage Topic Name

Description

The name of the Kafka topic which stores connector and task configurations.

Related Name

config.storage.topic

Default Value

connect-configs

API Name

config.storage.topic

Required

true

Cluster Group Id

Description

A unique name used to identify the Connect cluster group. The name specified here cannot conflict with consumer group IDs.

Related Name

group.id

Default Value

connect-cluster

API Name

group.id

Required

true

Include Connector Context In Logs

Description

If this is enabled, the log layout includes connector-specific and task-specific information in the log message, where appropriate. This makes it easier to identify those log messages that apply to a specific connector.

Related Name

include.connector.context

Default Value

true

API Name

include.connector.context

Required

false

Kafka Connect Configuration Directory

Description

Directory with all configurations for Kafka Connect daemons.

Related Name

kafka.connect.conf.directory

Default Value

$CONF_DIR

API Name

kafka.connect.conf.directory

Required

true

Java Home Path Override

Description

Java Home Path Override for Kafka Connect.

Related Name

kafka.connect.jdk.home

Default Value

API Name

kafka.connect.jdk.home

Required

false

Kafka Connect Heap Java Options

Description

Memory heap params while using Kafka Connect.

Related Name

KAFKA_HEAP_OPTS

Default Value

-Xms256M -Xmx2G

API Name

KAFKA_HEAP_OPTS

Required

false

Key Converter

Description

The key converter class used to convert between the Kafka Connect format and the serialized form that is written to Kafka. The key converter controls the format of the keys in the messages written to or read from Kafka. Since the key converter is independent of the connectors, it allows any connector to work with any serialization format. Examples of common formats include JSON and Avro.

Related Name

key.converter

Default Value

org.apache.kafka.connect.json.JsonConverter

API Name

key.converter

Required

true

Enable Key Converter Schema

Description

Enables the key converter to include schemas within each of the serialized keys.

Related Name

key.converter.schemas.enable

Default Value

true

API Name

key.converter.schemas.enable

Required

true

Jetty Metrics Port

Description

Jetty Metrics port to expose JMX Json.

Related Name

metrics.jetty.server.port

Default Value

28084

API Name

metrics.jetty.server.port

Required

true

Offset Flush Interval

Description

The interval, in milliseconds, at which Kafka Connect attempts to commit task offsets.

Related Name

offset.flush.interval.ms

Default Value

1 minute(s)

API Name

offset.flush.interval.ms

Required

true

Offset Storage Topic Replication Factor

Description

Replication factor used when creating the offset storage topic.

Related Name

offset.storage.replication.factor

Default Value

1

API Name

offset.storage.replication.factor

Required

true

Offset Storage Topic Name

Description

The name of the Kafka topic which stores connector offsets. If this topic does not exist, Kafka Connect will attempt to create it. Alternatively, you can also choose to create the topic manually before starting Kafka Connect.

Related Name

offset.storage.topic

Default Value

connect-offsets

API Name

offset.storage.topic

Required

true

Plugin Path

Description

Path to directories immediately containing jars with plugins and their dependencies, uber-jars with plugins and their dependencies and classes of plugins and their dependencies.

Related Name

plugin.path

Default Value

/var/lib/kafka

API Name

plugin.path

Required

false

Rest Extension Classes

Description

Comma-separated names of ConnectRestExtension classes, loaded and called in the order specified. Typically used to add custom capability like logging, security, etc.

Related Name

rest.extension.classes

Default Value

com.cloudera.dim.kafka.metrics.JmxJsonMetricsRestExtension

API Name

rest.extension.classes

Required

true

Kafka Connect Rest Port

Description

The port that the REST API listens on for connection requests. This port is used by Kafka Connect if TLS/SSL is disabled.

Related Name

rest.port

Default Value

28083

API Name

rest.port

Required

true

Secure Kafka Connect Rest Port

Description

The secure port that the REST API listens on for connection requests. This port is used by Kafka Connect if TLS/SSL is enabled.

Related Name

secure.rest.port

Default Value

28085

API Name

secure.rest.port

Required

true

SSL Client Authentication

Description

Client authentication mode for SSL connections. If set to "required", client authentication is required. If set to "requested", client authentication is requested and clients without certificates can still connect. If set to "none", which is the default value, no client authentication is required.

Related Name

ssl.client.auth

Default Value

none

API Name

ssl.client.auth

Required

false

Status Storage Topic Replication Factor

Description

Replication factor used when creating the offset storage topic.

Related Name

status.storage.replication.factor

Default Value

1

API Name

status.storage.replication.factor

Required

true

Status Storage Topic Name

Description

The name of the Kafka topic which stores connector and task status.

Related Name

status.storage.topic

Default Value

connect-status

API Name

status.storage.topic

Required

true

Value Converter

Description

The value converter class used to convert between the Kafka Connect format and the serialized form that is written to Kafka. The value converter controls the format of the values in the messages written to or read from Kafka. Since the value converter is independent of the connectors, it allows any connector to work with any serialization format. Examples of common formats include JSON and Avro.

Related Name

value.converter

Default Value

org.apache.kafka.connect.json.JsonConverter

API Name

value.converter

Required

true

Enable Value Converter Schema

Description

Enables the value converter to include schemas within each of the serialized values.

Related Name

value.converter.schemas.enable

Default Value

true

API Name

value.converter.schemas.enable

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Kafka Connect Prometheus Metrics Port

Description

Port for exposing Kafka Connect metrics as Prometheus metrics / OpenMetrics format.

Related Name

connect.prometheus.metrics.port

Default Value

28086

API Name

connect.prometheus.metrics.port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Kafka Connect TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Kafka Connect might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Kafka Connect TLS/SSL Trust Store Password

Description

The password for the Kafka Connect TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password.generator

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Kafka Connect

Description

Encrypt communication between clients and Kafka Connect using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Kafka Connect TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Kafka Connect is acting as a TLS/SSL server.

Related Name

ssl.key.password.generator

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Kafka Connect TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Kafka Connect is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Kafka Connect TLS/SSL Server Keystore File Password

Description

The password for the Kafka Connect keystore file.

Related Name

ssl.keystore.password.generator

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Bootstrap Servers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Bootstrap Servers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_bootstrap.servers

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Configuration Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Configuration Storage Topic Replication Factor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_config.storage.replication.factor

Required

true

Suppress Parameter Validation: Configuration Storage Topic Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Configuration Storage Topic Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_config.storage.topic

Required

true

Suppress Parameter Validation: Kafka Connect Advanced Configuration Snippet (Safety Valve) for connect-distributed.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Advanced Configuration Snippet (Safety Valve) for connect-distributed.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_connect-distributed.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka Connect Prometheus Metrics Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Prometheus Metrics Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_connect.prometheus.metrics.port

Required

true

Suppress Parameter Validation: Cluster Group Id

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cluster Group Id parameter.

Related Name

Default Value

false

API Name

role_config_suppression_group.id

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Kafka Connect Configuration Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Configuration Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.conf.directory

Required

true

Suppress Parameter Validation: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Home Path Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.jdk.home

Required

true

Suppress Parameter Validation: Kafka Connect Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_connect_role_env_safety_valve

Required

true

Suppress Parameter Validation: Kafka Connect Heap Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Heap Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_heap_opts

Required

true

Suppress Parameter Validation: Key Converter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Converter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_key.converter

Required

true

Suppress Parameter Validation: Kafka Connect Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Kafka Connect Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Jetty Metrics Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Jetty Metrics Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.jetty.server.port

Required

true

Suppress Parameter Validation: Offset Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Offset Storage Topic Replication Factor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_offset.storage.replication.factor

Required

true

Suppress Parameter Validation: Offset Storage Topic Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Offset Storage Topic Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_offset.storage.topic

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Plugin Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Plugin Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_plugin.path

Required

true

Suppress Parameter Validation: Rest Extension Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rest Extension Classes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rest.extension.classes

Required

true

Suppress Parameter Validation: Kafka Connect Rest Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Rest Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rest.port

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Secure Kafka Connect Rest Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Kafka Connect Rest Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_secure.rest.port

Required

true

Suppress Parameter Validation: Kafka Connect TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Kafka Connect TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Kafka Connect TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Kafka Connect TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Kafka Connect TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Status Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Status Storage Topic Replication Factor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_status.storage.replication.factor

Required

true

Suppress Parameter Validation: Status Storage Topic Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Status Storage Topic Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_status.storage.topic

Required

true

Suppress Parameter Validation: Value Converter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Value Converter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_value.converter

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_connect_unexpected_exits

Required

true

Kafka MirrorMaker

Advanced

Kafka MirrorMaker Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KAFKA_MIRROR_MAKER_role_env_safety_valve

Required

false

Kafka MirrorMaker Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_consumers.properties

Description

For advanced use only. A string to be inserted into mirror_maker_consumers.properties for this role only.

Related Name

Default Value

API Name

mirror_maker_consumers.properties_role_safety_valve

Required

false

Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_producers.properties

Description

For advanced use only. A string to be inserted into mirror_maker_producers.properties for this role only.

Related Name

Default Value

API Name

mirror_maker_producers.properties_role_safety_valve

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_client.properties

Description

For advanced use only. A string to be inserted into ssl_client.properties for this role only.

Related Name

Default Value

API Name

ssl_client.properties_role_safety_valve

Required

false

Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_server.properties

Description

For advanced use only. A string to be inserted into ssl_server.properties for this role only.

Related Name

Default Value

API Name

ssl_server.properties_role_safety_valve

Required

false

Logs

Kafka MirrorMaker Log Directory

Description

The log directory for log files of the role Kafka MirrorMaker.

Related Name

kafka_mirrormaker.log4j.dir

Default Value

/var/log/kafka

API Name

log_dir

Required

false

Kafka MirrorMaker Logging Threshold

Description

The minimum log level for Kafka MirrorMaker logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Kafka MirrorMaker Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Kafka MirrorMaker logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Kafka MirrorMaker Max Log Size

Description

The maximum size, in megabytes, per log file for Kafka MirrorMaker logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kafka_mirror_maker_fd_thresholds

Required

false

Kafka MirrorMaker Host Health Test

Description

When computing the overall Kafka MirrorMaker health, consider the host's health.

Related Name

Default Value

true

API Name

kafka_mirror_maker_host_health_enabled

Required

false

Kafka MirrorMaker Process Health Test

Description

Enables the health test that the Kafka MirrorMaker's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kafka_mirror_maker_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Abort on Send Failure

Description

Stop the entire mirror maker when a send failure occurs.

Related Name

abort.on.send.failure

Default Value

true

API Name

abort.on.send.failure

Required

false

Producer Batch Size

Description

This configuration controls the batch size in bytes. The producer will attempt to batch records together into fewer requests whenever multiple records are being sent to the same partition. This helps performance on both the client and the server.

Related Name

batch.size

Default Value

16 KiB

API Name

batch.size

Required

false

Destination Broker List

Description

Comma-separated list of IP:port (or hostname:port) pairs of brokers on destination cluster. This should be more than one, for high availability, but there's no need to list all brokers.

Related Name

bootstrap.servers

Default Value

API Name

bootstrap.servers

Required

true

Producer Buffer Memory

Description

The total bytes of memory the producer can use to buffer records waiting to be sent to the server.

Related Name

buffer.memory

Default Value

32 MiB

API Name

buffer.memory

Required

false

Producer Compression Type

Description

The compression type for all data generated by the producer.

Related Name

compression.type

Default Value

none

API Name

compression.type

Required

false

MirrorMaker Consumer Rebalance Listener

Description

A consumer rebalance listener of the ConsumerRebalanceListener type. Invoked when MirrorMaker's consumer rebalances.

Related Name

consumer.rebalance.listener

Default Value

API Name

consumer.rebalance.listener

Required

false

MirrorMaker Consumer Rebalance Listener Arguments

Description

Arguments used by MirrorMaker consumer rebalance listener.

Related Name

consumer.rebalance.listener.args

Default Value

API Name

consumer.rebalance.listener.args

Required

false

Consumer Request Timeout

Description

The maximum amount of time the consumer will wait for the response of a request. If the response is not received before the timeout elapses, the consumer will resend the request if necessary or fail the request if retries are exhausted.

Related Name

consumer.request.timeout.ms

Default Value

40 second(s)

API Name

consumer.request.timeout.ms

Required

false

Destination Kafka Cluster's Security Protocol

Description

Protocol used for communication with destination Kafka cluster.

Related Name

destination.security.protocol

Default Value

PLAINTEXT

API Name

destination.security.protocol

Required

false

Destination Kafka Cluster's Client Auth

Description

Only required if destination Kafka cluster requires client authentication.

Related Name

destination.ssl.client.auth

Default Value

false

API Name

destination.ssl.client.auth

Required

false

Consumer Minimum Fetch Size

Description

The minimum amount of data the server should return for a fetch request. If insufficient data is available, the request will wait for that much data to accumulate before answering the request. Setting this property to something greater than 1 will cause the server to wait for larger amounts of data to accumulate which can improve server throughput a bit at the cost of some additional latency.

Related Name

fetch.min.bytes

Default Value

1 B

API Name

fetch.min.bytes

Required

false

Consumer Group ID

Description

Name of the consumer group used by MirrorMaker. When multiple role instances are configured with the same topics and same group ID, the role instances load-balance replication for the topics. When multiple role instances are configured with the same topics but different group ID, each role instance replicates all the events for those topics - this can be used to replicate the source cluster into multiple destination clusters.

Related Name

group.id

Default Value

cloudera_mirrormaker

API Name

group.id

Required

false

Enable Authenticated Communication with the JMX Agent

Description

Enables Authenticated Communication with the JMX Agent.

Related Name

jmx.auth.enabled

Default Value

false

API Name

jmx.auth.enabled

Required

false

Name of User with Read-Write Access to the JMX Agent

Description

Specifies the name of the user that has read-write privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.control.user

Default Value

controlRole

API Name

jmx.control.user

Required

false

Password of user with read-write access to the JMX agent

Description

Specifies the password of the user that has read-write privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.control.user.passwd

Default Value

API Name

jmx.control.user.passwd

Required

false

Name of User with read-only access to the JMX Agent

Description

Specifies the name of the user that has read-only privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.monitor.user

Default Value

monitorRole

API Name

jmx.monitor.user

Required

false

Password of User with read-only Access to the JMX agent

Description

Specifies the password of the user that has read-only privileges when using password file-based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

jmx.monitor.user.passwd

Default Value

API Name

jmx.monitor.user.passwd

Required

false

Enable TLS client authentication for JMX port

Description

If enabled, a valid client certificate must be presented by the JMX client in order to connect to the JMX port. Ensure that the trusted CA certificates are present in either the ZooKeeper JMX TLS/SSL Server Trust Store file or the global trust store.

Related Name

jmx.ssl.client.auth.enabled

Default Value

false

API Name

jmx.ssl.client.auth.enabled

Required

false

Enable TLS/SSL for Kafka JMX

Description

Encrypt communication between clients and Kafka JMX using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

jmx.ssl.enabled

Default Value

false

API Name

jmx.ssl.enabled

Required

false

Producer Linger Time

Description

The upper bound on the delay for batching. Once the producer gets a batch.size worth of records for a partition it will be sent immediately regardless of this setting. However, if fewer than this many bytes accumulated for this partition the producer will 'linger' for the specified time waiting for more records to show up.

Related Name

linger.ms

Default Value

0 second(s)

API Name

linger.ms

Required

false

MirrorMaker Message Handler

Description

A MirrorMaker message handler of the MirrorMakerMessageHandler type that will process every record in-between producer and consumer.

Related Name

message.handler

Default Value

API Name

message.handler

Required

false

MirrorMaker Message Handler Arguments

Description

Arguments used by MirrorMaker message handler.

Related Name

message.handler.args

Default Value

API Name

message.handler.args

Required

false

Additional MirrorMaker Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags are passed here.

Related Name

mirror_maker_java_opts

Default Value

-server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -XX:G1HeapRegionSize=16M -XX:MinMetaspaceFreeRatio=50 -XX:MaxMetaspaceFreeRatio=80 -XX:+DisableExplicitGC -Djava.awt.headless=true -Djava.net.preferIPv4Stack=true -Dcom.sun.management.jmxremote.host=127.0.0.1 -Dcom.sun.management.jmxremote.local.only=true -Djava.rmi.server.hostname=127.0.0.1

API Name

mirror_maker_java_opts

Required

false

Java Heap Size of MirrorMaker

Description

Maximum size for the Java process heap memory. Passed to Java -Xmx. Measured in megabytes.

Related Name

mirror_maker_max_heap_size

Default Value

1 GiB

API Name

mirror_maker_max_heap_size

Required

false

Number of Consumer Threads

Description

Number of consumer threads.

Related Name

num.streams

Default Value

1

API Name

num.streams

Required

false

Offset Commit Interval

Description

Offset commit interval in milliseconds.

Related Name

offset.commit.interval.ms

Default Value

60000

API Name

offset.commit.interval.ms

Required

false

Producer Request Timeout

Description

The maximum amount of time the producer will wait for the response of a request. If the response is not received before the timeout elapses, the producer will resend the request if necessary or fail the request if retries are exhausted.

Related Name

producer.request.timeout.ms

Default Value

30 second(s)

API Name

producer.request.timeout.ms

Required

false

Consumer Session Timeout

Description

The timeout used to detect failures when using the group management facilities of Kafka. When the heartbeat of a consumer is not received within the session timeout, the broker will mark the consumer as failed and rebalance the group. Note that the value must be in the allowable range as configured in the broker by group.min.session.timeout.ms and group.max.session.timeout.ms.

Related Name

session.timeout.ms

Default Value

30 second(s)

API Name

session.timeout.ms

Required

false

Source Broker List

Description

Comma-separated list of IP:port (or hostname:port) pairs of brokers on source cluster. This should be more than one, for high availability, but there's no need to list all brokers.

Related Name

source.bootstrap.servers

Default Value

API Name

source.bootstrap.servers

Required

true

Source Kafka Cluster's Security Protocol

Description

Protocol used for communication with source Kafka cluster.

Related Name

source.security.protocol

Default Value

PLAINTEXT

API Name

source.security.protocol

Required

false

Source Kafka Cluster's Client Auth

Description

Only required if the source Kafka cluster requires client authentication.

Related Name

source.ssl.client.auth

Default Value

false

API Name

source.ssl.client.auth

Required

false

Topic Whitelist

Description

Regular expression that represents a set of topics to mirror.

Related Name

whitelist

Default Value

API Name

whitelist

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

JMX Port

Description

Port for JMX.

Related Name

jmx_port

Default Value

9394

API Name

jmx_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Kafka MirrorMaker TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Kafka MirrorMaker might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Kafka MirrorMaker TLS/SSL Trust Store Password

Description

The password for the Kafka MirrorMaker TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password.generator

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Kafka MirrorMaker

Description

Encrypt communication between clients and Kafka MirrorMaker using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Kafka MirrorMaker TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Kafka MirrorMaker is acting as a TLS/SSL server.

Related Name

ssl.key.password.generator

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Kafka MirrorMaker TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Kafka MirrorMaker is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Kafka MirrorMaker TLS/SSL Server Keystore File Password

Description

The password for the Kafka MirrorMaker keystore file.

Related Name

ssl.keystore.password.generator

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Destination Broker List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Destination Broker List parameter.

Related Name

Default Value

false

API Name

role_config_suppression_bootstrap.servers

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: MirrorMaker Consumer Rebalance Listener

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MirrorMaker Consumer Rebalance Listener parameter.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.rebalance.listener

Required

true

Suppress Parameter Validation: MirrorMaker Consumer Rebalance Listener Arguments

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MirrorMaker Consumer Rebalance Listener Arguments parameter.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.rebalance.listener.args

Required

true

Suppress Parameter Validation: Consumer Group ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Consumer Group ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_group.id

Required

true

Suppress Parameter Validation: Name of User with Read-Write Access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with Read-Write Access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user

Required

true

Suppress Parameter Validation: Password of user with read-write access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of user with read-write access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user.passwd

Required

true

Suppress Parameter Validation: Name of User with read-only access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with read-only access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user

Required

true

Suppress Parameter Validation: Password of User with read-only Access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of User with read-only Access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user.passwd

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: JMX Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_port

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_mirror_maker_role_env_safety_valve

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: MirrorMaker Message Handler

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MirrorMaker Message Handler parameter.

Related Name

Default Value

false

API Name

role_config_suppression_message.handler

Required

true

Suppress Parameter Validation: MirrorMaker Message Handler Arguments

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MirrorMaker Message Handler Arguments parameter.

Related Name

Default Value

false

API Name

role_config_suppression_message.handler.args

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_consumers.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_consumers.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_consumers.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Additional MirrorMaker Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional MirrorMaker Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_java_opts

Required

true

Suppress Parameter Validation: Java Heap Size of MirrorMaker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of MirrorMaker parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_max_heap_size

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_producers.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_producers.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_producers.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Source Broker List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Source Broker List parameter.

Related Name

Default Value

false

API Name

role_config_suppression_source.bootstrap.servers

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_client.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka MirrorMaker TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Kafka MirrorMaker TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_server.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_server.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Kafka MirrorMaker TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Kafka MirrorMaker TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Kafka MirrorMaker TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka MirrorMaker TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Topic Whitelist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Topic Whitelist parameter.

Related Name

Default Value

false

API Name

role_config_suppression_whitelist

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kafka_kafka_mirror_maker_unexpected_exits

Required

true

Service-Wide

Advanced

Kafka Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

KAFKA_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

kafka

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

kafka

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Kafka Broker Monitoring Thresholds

Description

The health test thresholds of the overall Kafka Broker health. The check returns "Concerning" health if the percentage of "Healthy" Kafka Brokers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kafka Brokers falls below the critical threshold.

Related Name

Default Value

Warning: 94.99 %, Critical: 49.99 %

API Name

KAFKA_KAFKA_BROKER_healthy_thresholds

Required

false

Healthy Kafka Connect Monitoring Thresholds

Description

The health test thresholds of the overall Kafka Connect health. The check returns "Concerning" health if the percentage of "Healthy" Kafka Connects falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Kafka Connects falls below the critical threshold.

Related Name

Default Value

Warning: 94.99 %, Critical: 49.99 %

API Name

KAFKA_KAFKA_CONNECT_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Atlas metadata namespace for Kafka Clients

Description

Metadata Namespace used in Atlas for Kafka clients (Producers, Consumers). It may be different from the topic namespace when clients used across clusters.

Related Name

atlas.metadata.namespace.client

Default Value

cm

API Name

atlas.metadata.namespace.client

Required

false

Atlas metadata namespace for Kafka Topics

Description

Metadata Namespace used in Atlas for Kafka topics.

Related Name

atlas.metadata.namespace.topic

Default Value

cm

API Name

atlas.metadata.namespace.topic

Required

false

Topic Auto Creation

Description

Enables auto creation of topics on the server. If set to true, it attempts to produce, consume, or fetch metadata for a non-existent topic automatically create the topic with the default replication factor and number of partitions.

Related Name

auto.create.topics.enable

Default Value

true

API Name

auto.create.topics.enable

Required

false

Enable Automatic Leader Rebalancing

Description

If automatic leader rebalancing is enabled, the controller tries to balance leadership for partitions among the brokers by periodically returning leadership for each partition to the preferred replica, if that replica is available.

Related Name

auto.leader.rebalance.enable

Default Value

true

API Name

auto.leader.rebalance.enable

Required

false

Enable Controlled Shutdown

Description

Enables controlled shutdown of the broker. If enabled, the broker moves all leaders on it to other brokers before shutting itself down. This reduces the unavailability window during shutdown.

Related Name

controlled.shutdown.enable

Default Value

true

API Name

controlled.shutdown.enable

Required

false

Controlled Shutdown Maximum Attempts

Description

Number of unsuccessful controlled shutdown attempts before executing an unclean shutdown. For example, the default value of 3 means that the system will attempt a controlled shutdown 3 times before executing an unclean shutdown.

Related Name

controlled.shutdown.max.retries

Default Value

3

API Name

controlled.shutdown.max.retries

Required

false

Default Replication Factor

Description

The default replication factor for automatically created topics.

Related Name

default.replication.factor

Default Value

1

API Name

default.replication.factor

Required

false

Enable Delegation Tokens

Description

Enables authentication with delegation tokens for this Kafka service. When enabled, a secure password is automatically generated and used as the "delegation.token.master.key" property for Kafka Brokers. Only allowed if Kerberos authentication is enabled.

Related Name

delegation.token.enable

Default Value

true

API Name

delegation.token.enable

Required

false

Delegation Token Expiry Time

Description

The expiry time of a delegation token. A delegation token can be renewed before its expiry time to extend its validity up to its maximum lifetime. If it is not renewed, it will expire even if it has time remaining from its maximum lifetime.

Related Name

delegation.token.expiry.time.ms

Default Value

1 day(s)

API Name

delegation.token.expiry.time.ms

Required

false

Delegation Token Maximum Lifetime

Description

The maximum amount of time that a delegation token can be valid for.

Related Name

delegation.token.max.lifetime.ms

Default Value

7 day(s)

API Name

delegation.token.max.lifetime.ms

Required

false

Enable Delete Topic

Description

Enables topic deletion using admin tools. When delete topic is disabled, deleting topics through the admin tools has no effect.

Related Name

delete.topic.enable

Default Value

true

API Name

delete.topic.enable

Required

false

Consumer Group Maximum Session Timeout

Description

The minimum allowed session timeout for registered consumers. Shorter timeouts result in quicker failure detection at the cost of more frequent consumer heartbeating, which can overwhelm broker resources.

Related Name

group.max.session.timeout.ms

Default Value

30 minute(s)

API Name

group.max.session.timeout.ms

Required

false

Consumer Group Minimum Session Timeout

Description

The minimum allowed session timeout for registered consumers. Shorter timeouts result in quicker failure detection at the cost of more frequent consumer heartbeating, which can overwhelm broker resources.

Related Name

group.min.session.timeout.ms

Default Value

6 second(s)

API Name

group.min.session.timeout.ms

Required

false

HDFS Service

Description

Name of the HDFS service that this Kafka service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

Enable Kafka Decommission

Description

Kafka decommission flag only takes affect when there is no Cruise Control. In other case the decommission will be always enabled.

Related Name

kafka.decommission.hook.enabled

Default Value

false

API Name

kafka.decommission.hook.enabled

Required

false

List of Metric Reporters

Description

List of metric reporter class names. HTTP reporter is included by default.

Related Name

kafka.metrics.reporters

Default Value

nl.techop.kafka.KafkaHttpMetricsReporter

API Name

kafka.metrics.reporters

Required

false

Enable Kerberos Authentication

Description

Enables Kerberos authentication for this Kafka service.

Related Name

kerberos.auth.enable

Default Value

false

API Name

kerberos.auth.enable

Required

false

LDAP URL

Description

The URL of LDAP for authenticating Kafka clients.

Related Name

ldap.auth.url

Default Value

API Name

ldap.auth.url

Required

false

LDAP User DN Template

Description

The LDAP user DN template for authenticating Kafka clients.

Related Name

ldap.auth.user.dn.template

Default Value

API Name

ldap.auth.user.dn.template

Required

false

Leader Imbalance Check Interval

Description

Defines the frequency of leader imbalance checks.

Related Name

leader.imbalance.check.interval.seconds

Default Value

5 minute(s)

API Name

leader.imbalance.check.interval.seconds

Required

false

Leader Imbalance Allowed Per Broker

Description

The percentage of leader imbalance allowed per broker. The controller rebalances leadership if the leader imbalance ratio goes above the configured value per broker.

Related Name

leader.imbalance.per.broker.percentage

Default Value

10 %

API Name

leader.imbalance.per.broker.percentage

Required

false

Log Cleaner Deduplication Buffer Size

Description

The total memory used for log deduplication across all cleaner threads. This memory is statically allocated and will not cause GC problems.

Related Name

log.cleaner.dedupe.buffer.size

Default Value

128 MiB

API Name

log.cleaner.dedupe.buffer.size

Required

false

Log Compaction Delete Record Retention Time

Description

The amount of time to retain delete messages for log compacted topics. Once a consumer has seen an original message, it has to be ensured that it also sees the delete message. If the delete message is removed too quickly, this might not happen. The configurable delete retention time helps to circumvent this issue.

Related Name

log.cleaner.delete.retention.ms

Default Value

7 day(s)

API Name

log.cleaner.delete.retention.ms

Required

false

Enable Log Compaction

Description

Enables the log cleaner to compact topics with cleanup.policy=compact on this cluster.

Related Name

log.cleaner.enable

Default Value

true

API Name

log.cleaner.enable

Required

false

Log Cleaner Clean Ratio

Description

Controls how frequently the log cleaner will attempt to clean the log. This ratio restricts the maximum space wasted by duplicates in the log. For example, if set to 0.5, then at most 50% of the log can be populated by duplicates. A higher ratio results in fewer, more efficient cleaning processes, but more wasted space in the log.

Related Name

log.cleaner.min.cleanable.ratio

Default Value

0.5

API Name

log.cleaner.min.cleanable.ratio

Required

false

Number of Log Cleaner Threads

Description

The number of background threads used for log cleaning.

Related Name

log.cleaner.threads

Default Value

1

API Name

log.cleaner.threads

Required

false

Log Flush Message Interval

Description

The number of messages written to a log partition before triggering an fsync on the log. Setting this property to a low value results in more frequent data to disk synchronization, but also has major impact on performance. For durability, Cloudera recommends the use of replication rather than depending on a single-server fsync. However, this setting can be used as an extra safety measure. If used in conjunction with log.flush.interval.ms, the log is flushed when either criteria is met.

Related Name

log.flush.interval.messages

Default Value

API Name

log.flush.interval.messages

Required

false

Log Flush Time Interval

Description

The maximum time between fsync calls on the log. If used in conjunction with log.flush.interval.messages, the log is flushed when either criteria is met.

Related Name

log.flush.interval.ms

Default Value

API Name

log.flush.interval.ms

Required

false

Log Flush Scheduler Interval

Description

The frequency, in milliseconds, with which the log flusher checks whether any log is eligible to be flushed to disk.

Related Name

log.flush.scheduler.interval.ms

Default Value

API Name

log.flush.scheduler.interval.ms

Required

false

Maximum Message Size

Description

The maximum size of a message that the server can receive. This property has to be in sync with the maximum fetch size the consumers use. Otherwise, an unruly producer could publish messages that are too large for consumption.

Related Name

message.max.bytes

Default Value

1000000 B

API Name

message.max.bytes

Required

false

Minimum Number of Replicas in ISR

Description

The minimum number of replicas in the in-sync replica needed to satisfy a produce request where required.acks=-1 (that is, all).

Related Name

min.insync.replicas

Default Value

1

API Name

min.insync.replicas

Required

false

Enable Kafka Monitoring

Description

Enables Kafka monitoring.

Related Name

monitoring.enabled

Default Value

true

API Name

monitoring.enabled

Required

false

Default Number of Partitions

Description

The default number of partitions for automatically created topics.

Related Name

num.partitions

Default Value

1

API Name

num.partitions

Required

false

Number of Replica Fetchers

Description

Number of threads used to replicate messages from leaders. Increasing this value increases the degree of I/O parallelism in the follower broker.

Related Name

num.replica.fetchers

Default Value

4

API Name

num.replica.fetchers

Required

false

Offset Retention Time

Description

After a consumer group loses all its consumers (i.e. becomes empty) its offsets will be kept for this retention period before getting discarded. For standalone consumers (using manual assignment), offsets will be expired after the time of last commit plus this retention period.

Related Name

offsets.retention.minutes

Default Value

7 day(s)

API Name

offsets.retention.minutes

Required

false

Offset Commit Topic Number of Partitions

Description

The number of partitions for the offset commit topic. Changing this value after deployment is currently unsupported, therefore, Cloudera recommends using a higher number of partitions (for example, 100-200) for production.

Related Name

offsets.topic.num.partitions

Default Value

50

API Name

offsets.topic.num.partitions

Required

false

Offset Commit Topic Replication Factor

Description

The replication factor for the offset commit topic. A higher setting (for example, 3 or 4) is recommended in order to ensure higher availability. If the offsets topic is created when there are fewer brokers than the replication factor, then the offsets topic is created with fewer replicas.

Related Name

offsets.topic.replication.factor

Default Value

3

API Name

offsets.topic.replication.factor

Required

false

PAM Service

Description

The PAM service name for authenticating Kafka clients. This corresponds to the service name in the PAM configuration.

Related Name

pam.auth.service

Default Value

login

API Name

pam.auth.service

Required

false

Enable Producer Metrics

Description

Enables producer metrics

Related Name

producer.metrics.enable

Default Value

true

API Name

producer.metrics.enable

Required

false

Default Consumer Quota

Description

Any consumer distinguished by clientId/consumer group will get throttled if it fetches more bytes than this value per-second.

Related Name

quota.consumer.default

Default Value

API Name

quota.consumer.default

Required

false

Default Producer Quota

Description

Any producer distinguished by clientId will get throttled if it produces more bytes than this value per-second.

Related Name

quota.producer.default

Default Value

API Name

quota.producer.default

Required

false

Ranger Kafka Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_kafka_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/kafka

API Name

ranger_kafka_plugin_hdfs_audit_directory

Required

false

'Ranger service' name for this Kafka service

Description

Name of the 'Ranger service', that is used for authorization by this Kafka service. If this parameter is set to the placeholder value '{{GENERATED_RANGER_SERVICE_NAME}}', a generated service name will be used, and if necessary, created. The generated service name will refer to the name of the cluster and the name of this Kafka service. The name can consist of alphanumeric and '_' characters.

Related Name

ranger.plugin.kafka.service.name

Default Value

cm_kafka

API Name

ranger_plugin_kafka_service_name

Required

false

RANGER Service

Description

Name of the RANGER service that this Kafka service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Replica Maximum Fetch Size

Description

The maximum number of bytes to fetch for each partition in fetch requests that replicas send to the leader. This value should be larger than message.max.bytes.

Related Name

replica.fetch.max.bytes

Default Value

1 MiB

API Name

replica.fetch.max.bytes

Required

false

Allowed Replica Time Lag

Description

If a follower has not sent any fetch requests, nor has it consumed up to the leader's log end offset during this time, the leader removes the follower from the ISR set.

Related Name

replica.lag.time.max.ms

Default Value

30 second(s)

API Name

replica.lag.time.max.ms

Required

false

SASL/PLAIN Authentication

Description

Authentication method that the SASL/PLAIN mechanism uses to authenticate clients.

Related Name

sasl.plain.auth

Default Value

none

API Name

sasl.plain.auth

Required

false

Minimum Number of Replicas in ISR for Transaction State Log

Description

Overridden min.insync.replicas config for the transaction topic.

Related Name

transaction.state.log.min.isr

Default Value

2

API Name

transaction.state.log.min.isr

Required

false

Transaction State Log Replication Factor

Description

The replication factor for the transaction topic (set higher to ensure availability). Internal topic creation will fail until the cluster size meets this replication factor requirement.

Related Name

transaction.state.log.replication.factor

Default Value

3

API Name

transaction.state.log.replication.factor

Required

false

Enable Unclean Leader Election

Description

Enables replicas not in the ISR set to be elected as leader as a last resort, even though doing so might result in data loss.

Related Name

unclean.leader.election.enable

Default Value

false

API Name

unclean.leader.election.enable

Required

false

ZooKeeper Root

Description

The znode in ZooKeeper used as a root for this Kafka cluster. WARNING: Do not change this property following the initial launch of the Kafka service. Only configure this property during the initial setup phase, before starting the Kafka service for the first time. Updating the root znode on a Kafka service that has already been started does not copy over the original znodes to the new root. This causes Kafka to lose its operational metadata.

Related Name

zookeeper.chroot

Default Value

/kafka

API Name

zookeeper.chroot

Required

false

Enable Secure Connection to ZooKeeper

Description

Enables SSL/TLS for all connections to ZooKeeper. This applies only if 'Enable TLS/SSL for ZooKeeper' is enabled on the ZooKeeper service.

Related Name

zookeeper.secure.connection.enable

Default Value

true

API Name

zookeeper.secure.connection.enable

Required

false

ZooKeeper Session Timeout

Description

If the server fails to send a heartbeat to ZooKeeper within this period of time, it is considered dead. If set to a too low value, ZooKeeper might falsely consider a server dead. If set to a too high value, ZooKeeper might take too long to recognize a dead server.

Related Name

zookeeper.session.timeout.ms

Default Value

18 second(s)

API Name

zookeeper.session.timeout.ms

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Kafka service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

kafka

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: Advertised Host

Description

Whether to suppress configuration warnings produced by the Advertised Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_advertised.host.name

Required

true

Suppress Configuration Validator: Advertised Port

Description

Whether to suppress configuration warnings produced by the Advertised Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_advertised.port

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for atlas-application.properties

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for atlas-application.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas-application.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Destination Broker List

Description

Whether to suppress configuration warnings produced by the Destination Broker List configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_bootstrap.servers

Required

true

Suppress Configuration Validator: Broker ID

Description

Whether to suppress configuration warnings produced by the Broker ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_broker.id

Required

true

Suppress Configuration Validator: Additional Broker Java Options

Description

Whether to suppress configuration warnings produced by the Additional Broker Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_broker_java_opts

Required

true

Suppress Configuration Validator: Java Heap Size of Broker

Description

Whether to suppress configuration warnings produced by the Java Heap Size of Broker configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_broker_max_heap_size

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Configuration Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the Configuration Storage Topic Replication Factor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_config.storage.replication.factor

Required

true

Suppress Configuration Validator: Configuration Storage Topic Name

Description

Whether to suppress configuration warnings produced by the Configuration Storage Topic Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_config.storage.topic

Required

true

Suppress Configuration Validator: Kafka Connect Advanced Configuration Snippet (Safety Valve) for connect-distributed.properties

Description

Whether to suppress configuration warnings produced by the Kafka Connect Advanced Configuration Snippet (Safety Valve) for connect-distributed.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_connect-distributed.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Connect Prometheus Metrics Port

Description

Whether to suppress configuration warnings produced by the Kafka Connect Prometheus Metrics Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_connect.prometheus.metrics.port

Required

true

Suppress Configuration Validator: MirrorMaker Consumer Rebalance Listener

Description

Whether to suppress configuration warnings produced by the MirrorMaker Consumer Rebalance Listener configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.rebalance.listener

Required

true

Suppress Configuration Validator: MirrorMaker Consumer Rebalance Listener Arguments

Description

Whether to suppress configuration warnings produced by the MirrorMaker Consumer Rebalance Listener Arguments configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.rebalance.listener.args

Required

true

Suppress Configuration Validator: Consumer Group ID

Description

Whether to suppress configuration warnings produced by the Consumer Group ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_group.id

Required

true

Suppress Configuration Validator: Name of User with Read-Write Access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the Name of User with Read-Write Access to the JMX Agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user

Required

true

Suppress Configuration Validator: Password of user with read-write access to the JMX agent

Description

Whether to suppress configuration warnings produced by the Password of user with read-write access to the JMX agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.control.user.passwd

Required

true

Suppress Configuration Validator: Name of User with read-only access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the Name of User with read-only access to the JMX Agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user

Required

true

Suppress Configuration Validator: Password of User with read-only Access to the JMX agent

Description

Whether to suppress configuration warnings produced by the Password of User with read-only Access to the JMX agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx.monitor.user.passwd

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: JMX Port

Description

Whether to suppress configuration warnings produced by the JMX Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_port

Required

true

Suppress Configuration Validator: Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-client.conf

Description

Whether to suppress configuration warnings produced by the Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-client.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-conf/kafka-client.conf_client_config_safety_valve

Required

true

Suppress Configuration Validator: Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-ranger-repo.properties

Description

Whether to suppress configuration warnings produced by the Kafka Client Advanced Configuration Snippet (Safety Valve) for kafka-conf/kafka-ranger-repo.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-conf/kafka-ranger-repo.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka-monitoring.properties

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka-monitoring.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka-monitoring.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Connect Configuration Directory

Description

Whether to suppress configuration warnings produced by the Kafka Connect Configuration Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.conf.directory

Required

true

Suppress Configuration Validator: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the Java Home Path Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.jdk.home

Required

true

Suppress Configuration Validator: HTTP Metric Report Host

Description

Whether to suppress configuration warnings produced by the HTTP Metric Report Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.host

Required

true

Suppress Configuration Validator: HTTP Metric Report Password

Description

Whether to suppress configuration warnings produced by the HTTP Metric Report Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.password

Required

true

Suppress Configuration Validator: HTTP Metric Report Port

Description

Whether to suppress configuration warnings produced by the HTTP Metric Report Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.port

Required

true

Suppress Configuration Validator: HTTP Metric Report User

Description

Whether to suppress configuration warnings produced by the HTTP Metric Report User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.http.metrics.user

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka.properties

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for kafka.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Kafka Broker Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_broker_role_env_safety_valve

Required

true

Suppress Configuration Validator: Kafka Connect Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Kafka Connect Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_connect_role_env_safety_valve

Required

true

Suppress Configuration Validator: Kafka Connect Heap Java Options

Description

Whether to suppress configuration warnings produced by the Kafka Connect Heap Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_heap_opts

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka_mirror_maker_role_env_safety_valve

Required

true

Suppress Configuration Validator: Key Converter

Description

Whether to suppress configuration warnings produced by the Key Converter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_key.converter

Required

true

Suppress Configuration Validator: Data Directories

Description

Whether to suppress configuration warnings produced by the Data Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log.dirs

Required

true

Suppress Configuration Validator: Segment File Size

Description

Whether to suppress configuration warnings produced by the Segment File Size configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log.segment.bytes

Required

true

Suppress Configuration Validator: Kafka Broker Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Kafka Broker Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker Log Directory

Description

Whether to suppress configuration warnings produced by the Kafka Broker Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: MirrorMaker Message Handler

Description

Whether to suppress configuration warnings produced by the MirrorMaker Message Handler configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_message.handler

Required

true

Suppress Configuration Validator: MirrorMaker Message Handler Arguments

Description

Whether to suppress configuration warnings produced by the MirrorMaker Message Handler Arguments configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_message.handler.args

Required

true

Suppress Configuration Validator: Jetty Metrics Port

Description

Whether to suppress configuration warnings produced by the Jetty Metrics Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.jetty.server.port

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_consumers.properties

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_consumers.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_consumers.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Additional MirrorMaker Java Options

Description

Whether to suppress configuration warnings produced by the Additional MirrorMaker Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_java_opts

Required

true

Suppress Configuration Validator: Java Heap Size of MirrorMaker

Description

Whether to suppress configuration warnings produced by the Java Heap Size of MirrorMaker configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_max_heap_size

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_producers.properties

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for mirror_maker_producers.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mirror_maker_producers.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Number of I/O Threads

Description

Whether to suppress configuration warnings produced by the Number of I/O Threads configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_num.io.threads

Required

true

Suppress Configuration Validator: Number of Network Threads

Description

Whether to suppress configuration warnings produced by the Number of Network Threads configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_num.network.threads

Required

true

Suppress Configuration Validator: Number of Recovery Threads per data directory

Description

Whether to suppress configuration warnings produced by the Number of Recovery Threads per data directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_num.recovery.threads.per.data.dir

Required

true

Suppress Configuration Validator: Number of Alter Log Dir Threads

Description

Whether to suppress configuration warnings produced by the Number of Alter Log Dir Threads configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_num.replica.alter.log.dirs.threads

Required

true

Suppress Configuration Validator: Offset Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the Offset Storage Topic Replication Factor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_offset.storage.replication.factor

Required

true

Suppress Configuration Validator: Offset Storage Topic Name

Description

Whether to suppress configuration warnings produced by the Offset Storage Topic Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_offset.storage.topic

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Plugin Path

Description

Whether to suppress configuration warnings produced by the Plugin Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_plugin.path

Required

true

Suppress Configuration Validator: TCP Port

Description

Whether to suppress configuration warnings produced by the TCP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_port

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Kafka Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Kafka Plugin Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_conf_path

Required

true

Suppress Configuration Validator: Ranger Kafka Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kafka Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Kafka Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kafka Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Kafka Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kafka Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kafka_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Rest Extension Classes

Description

Whether to suppress configuration warnings produced by the Rest Extension Classes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rest.extension.classes

Required

true

Suppress Configuration Validator: Kafka Connect Rest Port

Description

Whether to suppress configuration warnings produced by the Kafka Connect Rest Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rest.port

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Secure Kafka Connect Rest Port

Description

Whether to suppress configuration warnings produced by the Secure Kafka Connect Rest Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_secure.rest.port

Required

true

Suppress Configuration Validator: Source Broker List

Description

Whether to suppress configuration warnings produced by the Source Broker List configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_source.bootstrap.servers

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for ssl.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_client.properties

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_client.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Kafka Broker TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Kafka Broker TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Kafka Broker TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: TLS/SSL Port

Description

Whether to suppress configuration warnings produced by the TLS/SSL Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_port

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_server.properties

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Advanced Configuration Snippet (Safety Valve) for ssl_server.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Kafka Broker TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Kafka Broker TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Kafka Broker TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Kafka Broker TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Kafka Broker TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Kafka Broker TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Status Storage Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the Status Storage Topic Replication Factor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_status.storage.replication.factor

Required

true

Suppress Configuration Validator: Status Storage Topic Name

Description

Whether to suppress configuration warnings produced by the Status Storage Topic Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_status.storage.topic

Required

true

Suppress Configuration Validator: Value Converter

Description

Whether to suppress configuration warnings produced by the Value Converter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_value.converter

Required

true

Suppress Configuration Validator: Topic Whitelist

Description

Whether to suppress configuration warnings produced by the Topic Whitelist configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_whitelist

Required

true

Suppress Configuration Validator: Kafka Broker Advanced Configuration Snippet (Safety Valve) for zookeeper-ssl.properties

Description

Whether to suppress configuration warnings produced by the Kafka Broker Advanced Configuration Snippet (Safety Valve) for zookeeper-ssl.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper-ssl.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Atlas metadata namespace for Kafka Clients

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas metadata namespace for Kafka Clients parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas.metadata.namespace.client

Required

true

Suppress Parameter Validation: Atlas metadata namespace for Kafka Topics

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas metadata namespace for Kafka Topics parameter.

Related Name

Default Value

false

API Name

service_config_suppression_atlas.metadata.namespace.topic

Required

true

Suppress Parameter Validation: Controlled Shutdown Maximum Attempts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Controlled Shutdown Maximum Attempts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_controlled.shutdown.max.retries

Required

true

Suppress Parameter Validation: Default Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Replication Factor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_default.replication.factor

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: List of Metric Reporters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the List of Metric Reporters parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kafka.metrics.reporters

Required

true

Suppress Configuration Validator: Kafka Broker Count Validator

Description

Whether to suppress configuration warnings produced by the Kafka Broker Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kafka_broker_count_validator

Required

true

Suppress Configuration Validator: Kafka Connect Count Validator

Description

Whether to suppress configuration warnings produced by the Kafka Connect Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kafka_connect_count_validator

Required

true

Suppress Configuration Validator: Kafka MirrorMaker Count Validator

Description

Whether to suppress configuration warnings produced by the Kafka MirrorMaker Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kafka_mirror_maker_count_validator

Required

true

Suppress Parameter Validation: Kafka Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kafka_service_env_safety_valve

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap.auth.url

Required

true

Suppress Parameter Validation: LDAP User DN Template

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User DN Template parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap.auth.user.dn.template

Required

true

Suppress Parameter Validation: Leader Imbalance Check Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Leader Imbalance Check Interval parameter.

Related Name

Default Value

false

API Name

service_config_suppression_leader.imbalance.check.interval.seconds

Required

true

Suppress Parameter Validation: Leader Imbalance Allowed Per Broker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Leader Imbalance Allowed Per Broker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_leader.imbalance.per.broker.percentage

Required

true

Suppress Parameter Validation: Maximum Message Size

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Maximum Message Size parameter.

Related Name

Default Value

false

API Name

service_config_suppression_message.max.bytes

Required

true

Suppress Parameter Validation: Minimum Number of Replicas in ISR

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Minimum Number of Replicas in ISR parameter.

Related Name

Default Value

false

API Name

service_config_suppression_min.insync.replicas

Required

true

Suppress Parameter Validation: Default Number of Partitions

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Number of Partitions parameter.

Related Name

Default Value

false

API Name

service_config_suppression_num.partitions

Required

true

Suppress Parameter Validation: Number of Replica Fetchers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Replica Fetchers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_num.replica.fetchers

Required

true

Suppress Parameter Validation: Offset Commit Topic Number of Partitions

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Offset Commit Topic Number of Partitions parameter.

Related Name

Default Value

false

API Name

service_config_suppression_offsets.topic.num.partitions

Required

true

Suppress Parameter Validation: Offset Commit Topic Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Offset Commit Topic Replication Factor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_offsets.topic.replication.factor

Required

true

Suppress Parameter Validation: PAM Service

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the PAM Service parameter.

Related Name

Default Value

false

API Name

service_config_suppression_pam.auth.service

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Kafka Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kafka Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kafka_plugin_hdfs_audit_directory

Required

true

Suppress Parameter Validation: 'Ranger service' name for this Kafka service

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the 'Ranger service' name for this Kafka service parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_kafka_service_name

Required

true

Suppress Parameter Validation: Replica Maximum Fetch Size

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replica Maximum Fetch Size parameter.

Related Name

Default Value

false

API Name

service_config_suppression_replica.fetch.max.bytes

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Transaction State Log Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Transaction State Log Replication Factor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_transaction.state.log.replication.factor

Required

true

Suppress Parameter Validation: ZooKeeper Root

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Root parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper.chroot

Required

true

Suppress Parameter Validation: ZooKeeper Session Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Session Timeout parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper.session.timeout.ms

Required

true

Suppress Health Test: Kafka Broker Health

Description

Whether to suppress the results of the Kafka Broker Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_kafka_kafka_broker_healthy

Required

true

Suppress Health Test: Kafka Connect Health

Description

Whether to suppress the results of the Kafka Connect Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_kafka_kafka_connect_healthy

Required

true

Key Trustee Server Properties in Cloudera Runtime 7.2.18

Role groups:

Active Database

Advanced

Active Database Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

DB_ACTIVE_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

db_active_fd_thresholds

Required

false

Active Database Host Health Test

Description

When computing the overall Active Database health, consider the host's health.

Related Name

Default Value

true

API Name

db_active_host_health_enabled

Required

false

Active Database Process Health Test

Description

Enables the health test that the Active Database's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

db_active_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.

- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Database Storage Directory

Description

Directory (local file system) where the Key Trustee Server database will be stored. Changing this value after the service has been started will have no effect.

Related Name

db_root

Default Value

/var/lib/keytrustee/db

API Name

db_root

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Key Trustee Server Database Port

Description

The Key Trustee Server database server port. Changing this value after the service has been started will have no effect.

Related Name

db_port

Default Value

11381

API Name

db_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Active Database Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Database Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_active_role_env_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Database Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_port

Required

true

Suppress Parameter Validation: Database Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_root

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_host_health

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_active_unexpected_exits

Required

true

Active Key Trustee Server

Advanced

Active Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KEYTRUSTEE_ACTIVE_SERVER_role_env_safety_valve

Required

false

Active Key Trustee Server XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Active Key Trustee Server, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

For advanced use only. A string to be inserted into logging.conf for this role only.

Related Name

Default Value

API Name

logging.conf_role_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

For advanced use only. A string to be inserted into ssl.properties for this role only.

Related Name

Default Value

API Name

ssl.properties_role_safety_valve

Required

false

Logs

Active Key Trustee Server Log Directory

Description

The log directory for log files of the role Active Key Trustee Server.

Related Name

log_dir

Default Value

/var/lib/keytrustee/logs

API Name

log_dir

Required

false

Active Key Trustee Server Logging Threshold

Description

The minimum log level for Active Key Trustee Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Active Key Trustee Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Active Key Trustee Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Active Key Trustee Server Max Log Size

Description

The maximum size, in megabytes, per log file for Active Key Trustee Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

keytrustee_active_server_fd_thresholds

Required

false

Active Key Trustee Server Host Health Test

Description

When computing the overall Active Key Trustee Server health, consider the host's health.

Related Name

Default Value

true

API Name

keytrustee_active_server_host_health_enabled

Required

false

Active Key Trustee Server Process Health Test

Description

Enables the health test that the Active Key Trustee Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

keytrustee_active_server_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

KeyTrustee Server Active Database Port

Description

Port used by Active Database role in KeyTrustee Server.

Related Name

db_port

Default Value

11381

API Name

db_port

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Key Trustee Server Port

Description

The Key Trustee Server port number.

Related Name

keytrustee_port

Default Value

11371

API Name

keytrustee_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Active Key Trustee Server TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Active Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

ssl.cacert.location

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Active Key Trustee Server TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Active Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl.cert.location

Default Value

/var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee.pem

API Name

ssl_server_certificate_location

Required

false

Active Key Trustee Server TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Active Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl.privatekey.location

Default Value

/var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee-pk.pem

API Name

ssl_server_privatekey_location

Required

false

Active Key Trustee Server TLS/SSL Private Key Password

Description

The password for the private key in the Active Key Trustee Server TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

ssl.privatekey.password

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Active Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_active_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_port

Required

true

Suppress Parameter Validation: Active Key Trustee Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Active Key Trustee Server XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logging.conf_role_safety_valve

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Active Key Trustee Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Active Key Trustee Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Active Key Trustee Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Active Key Trustee Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_active_server_unexpected_exits

Required

true

Passive Database

Advanced

Passive Database Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

DB_PASSIVE_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

db_passive_fd_thresholds

Required

false

Passive Database Host Health Test

Description

When computing the overall Passive Database health, consider the host's health.

Related Name

Default Value

true

API Name

db_passive_host_health_enabled

Required

false

Passive Database Process Health Test

Description

Enables the health test that the Passive Database's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

db_passive_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.

- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Database Storage Directory

Description

Directory (local file system) where the Key Trustee Server database will be stored. Changing this value after the service has been started will have no effect.

Related Name

db_root

Default Value

/var/lib/keytrustee/db

API Name

db_root

Required

false

Retry Attempts

Description

Number of times a connection attempt will be made before giving up.

Related Name

retry_attempts

Default Value

30

API Name

retry_attempts

Required

true

Retry Timeout

Description

Number of secconds to wait between retries.

Related Name

retry_timeout

Default Value

1 second(s)

API Name

retry_timeout

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Key Trustee Server Database Port

Description

The Key Trustee Server database server port. Changing this value after the service has been started will have no effect.

Related Name

db_port

Default Value

11381

API Name

db_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Passive Database Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Database Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_passive_role_env_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Database Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_port

Required

true

Suppress Parameter Validation: Database Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_db_root

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Retry Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Retry Timeout parameter.

Related Name

Default Value

false

API Name

role_config_suppression_retry_timeout

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_host_health

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_db_passive_unexpected_exits

Required

true

Passive Key Trustee Server

Advanced

Passive Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KEYTRUSTEE_PASSIVE_SERVER_role_env_safety_valve

Required

false

Passive Key Trustee Server XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Passive Key Trustee Server, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

For advanced use only. A string to be inserted into logging.conf for this role only.

Related Name

Default Value

API Name

logging.conf_role_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

For advanced use only. A string to be inserted into ssl.properties for this role only.

Related Name

Default Value

API Name

ssl.properties_role_safety_valve

Required

false

Logs

Passive Key Trustee Server Log Directory

Description

The log directory for log files of the role Passive Key Trustee Server.

Related Name

log_dir

Default Value

/var/lib/keytrustee/logs

API Name

log_dir

Required

false

Passive Key Trustee Server Logging Threshold

Description

The minimum log level for Passive Key Trustee Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Passive Key Trustee Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Passive Key Trustee Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Passive Key Trustee Server Max Log Size

Description

The maximum size, in megabytes, per log file for Passive Key Trustee Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

keytrustee_passive_server_fd_thresholds

Required

false

Passive Key Trustee Server Host Health Test

Description

When computing the overall Passive Key Trustee Server health, consider the host's health.

Related Name

Default Value

true

API Name

keytrustee_passive_server_host_health_enabled

Required

false

Passive Key Trustee Server Process Health Test

Description

Enables the health test that the Passive Key Trustee Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

keytrustee_passive_server_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Key Trustee Server Port

Description

The Key Trustee Server port number.

Related Name

keytrustee_port

Default Value

11371

API Name

keytrustee_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Passive Key Trustee Server TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Passive Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

ssl.cacert.location

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Passive Key Trustee Server TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Passive Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl.cert.location

Default Value

/var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee.pem

API Name

ssl_server_certificate_location

Required

false

Passive Key Trustee Server TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Passive Key Trustee Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl.privatekey.location

Default Value

/var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee-pk.pem

API Name

ssl_server_privatekey_location

Required

false

Passive Key Trustee Server TLS/SSL Private Key Password

Description

The password for the private key in the Passive Key Trustee Server TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

ssl.privatekey.password

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Passive Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_passive_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_port

Required

true

Suppress Parameter Validation: Passive Key Trustee Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Passive Key Trustee Server XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logging.conf_role_safety_valve

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Passive Key Trustee Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Passive Key Trustee Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Passive Key Trustee Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Passive Key Trustee Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_keytrustee_server_keytrustee_passive_server_unexpected_exits

Required

true

Service-Wide

Advanced

Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

KEYTRUSTEE_SERVER_service_env_safety_valve

Required

false

Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

For advanced use only, a string to be inserted into logging.conf. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

logging.conf_service_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

keytrustee

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

keytrustee

API Name

process_username

Required

true

Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

For advanced use only, a string to be inserted into ssl.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ssl.properties_service_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Supported Cipher Configuration for SSL

Description

A list of allowed and disallowed ciphers, colon-separated (':'). Using a exclamation mark ('!') in front of the cipher name will disallow the respective cipher. For cipher options check OpenSSL cipher list. If blank then default ciphers are set.

Related Name

ciphers

Default Value

API Name

ciphers

Required

false

Key Trustee Home

Description

Home directory of Key Trustee.

Related Name

keytrustee.home

Default Value

/var/lib/keytrustee/.keytrustee

API Name

keytrustee.home

Required

false

Minimum TLS Support

Description

Minimum TLS protocol supported.

Related Name

tls.min.protocols

Default Value

TLSv1

API Name

tls.min.protocols

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Active Database Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Active Database Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_db_active_role_env_safety_valve

Required

true

Suppress Configuration Validator: Passive Database Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Passive Database Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_db_passive_role_env_safety_valve

Required

true

Suppress Configuration Validator: Database Storage Directory

Description

Whether to suppress configuration warnings produced by the Database Storage Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_db_root

Required

true

Suppress Configuration Validator: Active Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_active_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Passive Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Passive Key Trustee Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_passive_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Key Trustee Server Port

Description

Whether to suppress configuration warnings produced by the Key Trustee Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_port

Required

true

Suppress Configuration Validator: Active Key Trustee Server Log Directory

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Active Key Trustee Server XML Override

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server XML Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Configuration Validator: Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for logging.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logging.conf_role_safety_valve

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Retry Timeout

Description

Whether to suppress configuration warnings produced by the Retry Timeout configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_retry_timeout

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server Advanced Configuration Snippet (Safety Valve) for ssl.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Active Key Trustee Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server TLS/SSL Server CA Certificate (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Configuration Validator: Active Key Trustee Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Configuration Validator: Active Key Trustee Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Configuration Validator: Active Key Trustee Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Parameter Validation: Supported Cipher Configuration for SSL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Supported Cipher Configuration for SSL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ciphers

Required

true

Suppress Configuration Validator: Active Database Count Validator

Description

Whether to suppress configuration warnings produced by the Active Database Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_db_active_count_validator

Required

true

Suppress Configuration Validator: Passive Database Count Validator

Description

Whether to suppress configuration warnings produced by the Passive Database Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_db_passive_count_validator

Required

true

Suppress Parameter Validation: Key Trustee Home

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Home parameter.

Related Name

Default Value

false

API Name

service_config_suppression_keytrustee.home

Required

true

Suppress Configuration Validator: Active Key Trustee Server Count Validator

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_keytrustee_active_server_count_validator

Required

true

Suppress Configuration Validator: Passive Key Trustee Server Count Validator

Description

Whether to suppress configuration warnings produced by the Passive Key Trustee Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_keytrustee_passive_server_count_validator

Required

true

Suppress Parameter Validation: Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_keytrustee_server_service_env_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for logging.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for logging.conf parameter.

Related Name

Default Value

false

API Name

service_config_suppression_logging.conf_service_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for ssl.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Service Advanced Configuration Snippet (Safety Valve) for ssl.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl.properties_service_safety_valve

Required

true

Key-Value Store Indexer Properties in Cloudera Runtime 7.2.18

Role groups:

Lily HBase Indexer

Advanced

Lily HBase Indexer Advanced Configuration Snippet (Safety Valve) for hbase-indexer-site.xml

Description

For advanced use only. A string to be inserted into hbase-indexer-site.xml for this role only.

Related Name

Default Value

API Name

hbase_indexer_config_safety_valve

Required

false

Java Configuration Options for Lily HBase Indexer

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

hbase_indexer_java_opts

Required

false

System Group

Description

The group that the HBase Indexer process should run as.

Related Name

Default Value

hbase

API Name

hbase_indexer_process_groupname

Required

true

System User

Description

The user that the HBase Indexer process should run as.

Related Name

Default Value

hbase

API Name

hbase_indexer_process_username

Required

true

Lily HBase Indexer Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HBASE_INDEXER_role_env_safety_valve

Required

false

HBase Indexer ZooKeeper Session Timeout

Description

ZooKeeper session timeout. Controls the amount of time the HBase Indexer will attempt to connect to ZooKeeper before timing out.

Related Name

hbaseindexer.zookeeper.session.timeout

Default Value

1 minute(s)

API Name

hbase_indexer_zk_session_timeout

Required

false

Lily HBase Indexer Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

HBase Indexer Log Directory

Description

Directory where HBase Indexer will place its log files.

Related Name

Default Value

/var/log/hbase-solr

API Name

hbase_indexer_log_dir

Required

true

Lily HBase Indexer Logging Threshold

Description

The minimum log level for Lily HBase Indexer logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Lily HBase Indexer Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Lily HBase Indexer logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Lily HBase Indexer Max Log Size

Description

The maximum size, in megabytes, per log file for Lily HBase Indexer logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hbase_indexer_fd_thresholds

Required

false

Lily HBase Indexer Host Health Test

Description

When computing the overall Lily HBase Indexer health, consider the host's health.

Related Name

Default Value

true

API Name

hbase_indexer_host_health_enabled

Required

false

Lily HBase Indexer Process Health Test

Description

Enables the health test that the Lily HBase Indexer's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hbase_indexer_scm_health_enabled

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.

- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

HBase Indexer HTTP Port

Description

HTTP port used by HBase Indexer.

Related Name

hbaseindexer.http.port

Default Value

11060

API Name

hbase_indexer_http_port

Required

true

Resource Management

Java Heap Size of Lily HBase Indexer in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

hbase_indexer_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Lily HBase Indexer roles.

Related Name

Default Value

hbase

API Name

kerberos_role_princ_name

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Lily HBase Indexer Advanced Configuration Snippet (Safety Valve) for hbase-indexer-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Lily HBase Indexer Advanced Configuration Snippet (Safety Valve) for hbase-indexer-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_config_safety_valve

Required

true

Suppress Parameter Validation: HBase Indexer HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Indexer HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_http_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Lily HBase Indexer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Lily HBase Indexer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_java_opts

Required

true

Suppress Parameter Validation: HBase Indexer Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Indexer Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_log_dir

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_process_username

Required

true

Suppress Parameter Validation: Lily HBase Indexer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Lily HBase Indexer Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Lily HBase Indexer Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Lily HBase Indexer Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hbase_indexer_unexpected_exits

Required

true

Service-Wide

Advanced

Key-Value Store Indexer Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ks_indexer_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Lily HBase Indexer Monitoring Thresholds

Description

The health test thresholds of the overall Lily HBase Indexer health. The check returns "Concerning" health if the percentage of "Healthy" Lily HBase Indexers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Lily HBase Indexers falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

ks_indexer_indexers_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Morphlines

Custom Mime-types File

Description

Text that goes verbatim into custom-mimetypes.xml file used by HBase Indexers.

Related Name

Default Value

<!-- Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the License); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an AS IS BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either

express or implied. See the License for the specific language governing permissions and limitations under the License. --><mime-info> <mime-type type=text/space-separated-values> <glob pattern=*.ssv/> </mime-type> <mime-type type=avro/binary> <magic priority=50> <match offset=0 type=string value=0x4f626a01/> </magic> <glob pattern=*.avro/> </mime-type> <mime-type type=mytwittertest/json+delimited+length> <magic priority=50> <match offset=0:16 type=regex value=[0-9]+(\r)?\n\\"/> </magic> </mime-type> <mime-type type=application/hadoop-sequence-file> <magic priority=50> <match offset=0 type=regex value=SEQ[\0-\6]/> </magic> </mime-type> </mime-info>

API Name

custom_mimetypes_file

Required

false

Grok Dictionary File

Description

Text that goes verbatim into grok-dictionary.conf file used by HBase Indexers.

Related Name

Default Value

USERNAME [a-zA-Z0-9._-]+ USER %USERNAME INT (?:[+-]?(?:[0-9]+)) BASE10NUM (?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+))) NUMBER (?:%BASE10NUM) BASE16NUM (?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+)) BASE16FLOAT \b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]*)?)|(?:\.[0-9A-Fa-f]+)))\b POSINT \b(?:[1-9][0-9]*)\b NONNEGINT \b(?:[0-9]+)\b WORD \b\w+\b NOTSPACE \S+ SPACE \s* DATA .*? GREEDYDATA .* #QUOTEDSTRING (?:(?<!\\)(?:(?:\\.|[^\\])*|(?:'(?:\\.|[^\\'])*')|(?:`(?:\\.|[^\\`])*`))) QUOTEDSTRING (?>(?<!\\)(?>(?>\\.|[^\\]+)+||(?>'(?>\\.|[^\\']+)+')|''|(?>`(?>\\.|[^\\`]+)+`)|``)) UUID [A-Fa-f0-9]8-(?:[A-Fa-f0-9]4-)3[A-Fa-f0-9]12 # Networking MAC (?:%CISCOMAC|%WINDOWSMAC|%COMMONMAC) CISCOMAC (?:(?:[A-Fa-f0-9]4\.)2[A-Fa-f0-9]4) WINDOWSMAC (?:(?:[A-Fa-f0-9]2-)5[A-Fa-f0-9]2) COMMONMAC (?:(?:[A-Fa-f0-9]2:)5[A-Fa-f0-9]2) IP (?<![0-9])(?:(?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]1, 2)[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]1, 2)[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]1, 2)[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]1, 2))(?![0-9]) HOSTNAME \b(?:[0-9A-Za-z][0-9A-Za-z-]0, 62)(?:\.(?:[0-9A-Za-z][0-9A-Za-z-]0, 62))*(\.?|\b) HOST %HOSTNAME IPORHOST (?:%HOSTNAME|%IP) #HOSTPORT (?:%IPORHOST=~/\./:%POSINT) # WH # paths PATH (?:%UNIXPATH|%WINPATH) UNIXPATH (?>/(?>[\w_%!$@:., -]+|\\.)*)+ #UNIXPATH (?<![\w\/])(?:/[^\/\s?*]*)+ LINUXTTY (?>/dev/pts/%NONNEGINT) BSDTTY (?>/dev/tty[pq][a-z0-9]) TTY (?:%BSDTTY|%LINUXTTY) WINPATH (?>[A-Za-z]+:|\\)(?:\\[^\\?*]*)+ URIPROTO [A-Za-z]+(\+[A-Za-z+]+)? URIHOST %IPORHOST(?::%POSINT:port)? # uripath comes loosely from RFC1738, but mostly from what Firefox # doesn't turn into %XX URIPATH (?:/[A-Za-z0-9$.+!*'(), ~:;=#%_\-]*)+ #URIPARAM \?(?:[A-Za-z0-9]+(?:=(?:[^&]*))?(?:&(?:[A-Za-z0-9]+(?:=(?:[^&]*))?)?)*)? URIPARAM \?[A-Za-z0-9$.+!*'|(), ~#%&/=:;_?\-\[\]]* URIPATHPARAM %URIPATH(?:%URIPARAM)? URI %URIPROTO://(?:%USER(?::[^@]*)?@)?(?:%URIHOST)?(?:%URIPATHPARAM)? # Months: January, Feb, 3, 03, 12, December MONTH \b(?:Jan(?:uary)?|Feb(?:ruary)?|Mar(?:ch)?|Apr(?:il)?|May|Jun(?:e)?|Jul(?:y)?|Aug(?:ust)?|Sep(?:tember)?|Oct(?:ober)?|Nov(?:ember)?|Dec(?:ember)?)\b MONTHNUM (?:0?[1-9]|1[0-2]) MONTHDAY (?:(?:0[1-9])|(?:[12][0-9])|(?:3[01])|[1-9]) # Days: Monday, Tue, Thu, etc... DAY (?:Mon(?:day)?|Tue(?:sday)?|Wed(?:nesday)?|Thu(?:rsday)?|Fri(?:day)?|Sat(?:urday)?|Sun(?:day)?) # Years? YEAR (?>\d\d)1, 2 # Time: HH:MM:SS #TIME \d2:\d2(?::\d2(?:\.\d+)?)? # I'm still on the fence about using grok to perform the time match, # since it's probably slower. # TIME %POSINT<24:%POSINT<60(?::%POSINT<60(?:\.%POSINT)?)? HOUR (?:2[0123]|[01]?[0-9]) MINUTE (?:[0-5][0-9]) # '60' is a leap second in most time standards and thus is valid. SECOND (?:(?:[0-5][0-9]|60)(?:[:.,][0-9]+)?) TIME (?!<[0-9])%HOUR:%MINUTE(?::%SECOND)(?![0-9]) # datestamp is YYYY/MM/DD-HH:MM:SS.UUUU (or something like it) DATE_US %MONTHNUM[/-]%MONTHDAY[/-]%YEAR DATE_EU %MONTHDAY[./-]%MONTHNUM[./-]%YEAR ISO8601_TIMEZONE (?:Z|

[+-]%HOUR(?::?%MINUTE)) ISO8601_SECOND (?:%SECOND|60) TIMESTAMP_ISO8601 %YEAR-%MONTHNUM-%MONTHDAY[T]%HOUR:?%MINUTE(?::?%SECOND)? %ISO8601_TIMEZONE? DATE %DATE_US|%DATE_EU DATESTAMP %DATE[-]%TIME TZ (?:[PMCE][SD]T) DATESTAMP_RFC822 %DAY %MONTH %MONTHDAY %YEAR %TIME %TZ DATESTAMP_OTHER %DAY %MONTH %MONTHDAY %TIME %TZ %YEAR # Syslog Dates: Month Day HH:MM:SS SYSLOGTIMESTAMP %MONTH + %MONTHDAY %TIME PROG (?:[\w._/%-]+) SYSLOGPROG %PROG:program(?:\[%POSINT:pid\])? SYSLOGHOST %IPORHOST SYSLOGFACILITY <%NONNEGINT:facility.%NONNEGINT:priority> HTTPDATE %MONTHDAY/%MONTH/%YEAR: %TIME %INT # Shortcuts QS %QUOTEDSTRING # Log formats SYSLOGBASE %SYSLOGTIMESTAMP:timestamp (?:%SYSLOGFACILITY)?%SYSLOGHOST:logsource %SYSLOGPROG: COMBINEDAPACHELOG %IPORHOST:clientip %USER:ident %USER:auth \[%HTTPDATE:timestamp\] (?:%WORD:verb %NOTSPACE:request(?: HTTP/%NUMBER:httpversion)?|%DATA:rawrequest) %NUMBER:response (?:%NUMBER:bytes|-) %QS:referrer %QS:agent # Log Levels LOGLEVEL ([T|t]race|TRACE|[D|d]ebug|DEBUG|[N|n]otice|NOTICE|[I|i]nfo|INFO|[W|w]arn?(?:ing)?|WARN?(?:ING)?|[E|e]rr?(?:or)?|ERR?(?:OR)?|[C|c]rit?(?:ical)?|CRIT?(?:ICAL)?|[F|f]atal|FATAL|[S|s]evere|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)

API Name

grok_dictionary_conf_file

Required

false

Morphlines File

Description

Text that goes into morphlines.conf file used by HBase Indexers. The text goes verbatim into the config file except that $ZK_HOST is replaced by the ZooKeeper quorum of the Solr service.

Related Name

Default Value

SOLR_LOCATOR : # Name of solr collection collection : collection # ZooKeeper ensemble zkHost : $ZK_HOST morphlines : [id : morphline importCommands : [org.kitesdk.**, com.ngdata.**] commands : [extractHBaseCells mappings : [inputColumn : data:* outputField : data type : string source : value] logDebug format : output record: , args : [@]]]

API Name

morphlines_conf_file

Required

false

Other

HBase Service

Description

Name of the HBase service that this Key-Value Store Indexer service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

true

Solr Service

Description

Name of the Solr service that this Key-Value Store Indexer service instance depends on

Related Name

Default Value

API Name

solr_service

Required

true

Security

HBase Indexer Secure Authentication

Description

Authentication mechanism used by HBase Indexer.

Related Name

hbaseindexer.authentication.type

Default Value

simple

API Name

hbase_indexer_security_authentication

Required

false

HBase Indexer TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HBase Indexer might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

keystore_indexer_truststore_file

Required

false

HBase Indexer TLS/SSL Trust Store Password

Description

The password for the HBase Indexer TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

keystore_indexer_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Lily HBase Indexer Advanced Configuration Snippet (Safety Valve) for hbase-indexer-site.xml

Description

Whether to suppress configuration warnings produced by the Lily HBase Indexer Advanced Configuration Snippet (Safety Valve) for hbase-indexer-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_config_safety_valve

Required

true

Suppress Configuration Validator: HBase Indexer HTTP Port

Description

Whether to suppress configuration warnings produced by the HBase Indexer HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_http_port

Required

true

Suppress Configuration Validator: Java Configuration Options for Lily HBase Indexer

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Lily HBase Indexer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_java_opts

Required

true

Suppress Configuration Validator: HBase Indexer Log Directory

Description

Whether to suppress configuration warnings produced by the HBase Indexer Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_log_dir

Required

true

Suppress Configuration Validator: System Group

Description

Whether to suppress configuration warnings produced by the System Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_process_groupname

Required

true

Suppress Configuration Validator: System User

Description

Whether to suppress configuration warnings produced by the System User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_process_username

Required

true

Suppress Configuration Validator: Lily HBase Indexer Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Lily HBase Indexer Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hbase_indexer_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the Role-Specific Kerberos Principal configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Configuration Validator: Lily HBase Indexer Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Lily HBase Indexer Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Custom Mime-types File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Mime-types File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_custom_mimetypes_file

Required

true

Suppress Parameter Validation: Grok Dictionary File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Grok Dictionary File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_grok_dictionary_conf_file

Required

true

Suppress Configuration Validator: Lily HBase Indexer Count Validator

Description

Whether to suppress configuration warnings produced by the Lily HBase Indexer Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hbase_indexer_count_validator

Required

true

Suppress Parameter Validation: HBase Indexer TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Indexer TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_keystore_indexer_truststore_file

Required

true

Suppress Parameter Validation: HBase Indexer TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HBase Indexer TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_keystore_indexer_truststore_password

Required

true

Suppress Parameter Validation: Key-Value Store Indexer Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key-Value Store Indexer Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ks_indexer_env_safety_valve

Required

true

Suppress Parameter Validation: Morphlines File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Morphlines File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_morphlines_conf_file

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Lily HBase Indexer Health

Description

Whether to suppress the results of the Lily HBase Indexer Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ks_indexer_hbase_indexers_healthy

Required

true

Knox Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/knox

API Name

client_config_root_dir

Required

true

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Knox Gateway

Advanced

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties

Description

For advanced use only. A string to be inserted into conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties for this role only.

Related Name

Default Value

API Name

conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy.properties

Description

For advanced use only. A string to be inserted into conf/auto-discovery-advanced-configuration-cdp-proxy.properties for this role only.

Related Name

Default Value

API Name

conf/auto-discovery-advanced-configuration-cdp-proxy.properties_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/cdp-resources.xml

Description

For advanced use only. A string to be inserted into conf/cdp-resources.xml for this role only.

Related Name

Default Value

API Name

conf/cdp-resources.xml_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

For advanced use only. A string to be inserted into conf/gateway-site.xml for this role only.

Related Name

Default Value

API Name

conf/gateway-site.xml_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-audit.xml

Description

For advanced use only. A string to be inserted into conf/ranger-knox-audit.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-knox-audit.xml_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-knox-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-knox-policymgr-ssl.xml_role_safety_valve

Required

false

Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-security.xml

Description

For advanced use only. A string to be inserted into conf/ranger-knox-security.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-knox-security.xml_role_safety_valve

Required

false

Knox Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KNOX_GATEWAY_role_env_safety_valve

Required

false

Knox Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Knox Gateway Log Directory

Description

The log directory for log files of the role Knox Gateway.

Related Name

log_dir

Default Value

/var/log/knox/gateway

API Name

log_dir

Required

false

Knox Gateway Logging Threshold

Description

The minimum log level for Knox Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Knox Gateway Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Knox Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Knox Gateway Max Log Size

Description

The maximum size, in megabytes, per log file for Knox Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

knox_gateway_fd_thresholds

Required

false

Knox Gateway Host Health Test

Description

When computing the overall Knox Gateway health, consider the host's health.

Related Name

Default Value

true

API Name

knox_gateway_host_health_enabled

Required

false

Knox Gateway Process Health Test

Description

Enables the health test that the Knox Gateway's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

knox_gateway_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Knox Gateway Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Knox Simplified Topology Management - API Authentication Provider

Description

Authentication provider declaration used by pre-deinfed topologies such as admin, metadata or cdp-proxy-api.

Related Name

gateway_api_authentication_provider

Default Value

role=authentication authentication.name=ShiroProvider authentication.param.sessionTimeout=30 authentication.param.main.pamRealm=org.apache.knox.gateway.shirorealm.KnoxPamRealm authentication.param.main.pamRealm.service=login authentication.param.urls./**=authcBasic

API Name

gateway_api_authentication_provider

Required

false

Auto Discovery - Advanced Configuration Monitoring Interval

Description

Defines the frequency of Knox's service auto-discovery advanced configuration files (auto-discovery-advanced-configuration-[cdp-proxy|cdp-proxy-api].properties) monitoring.

Related Name

gateway.cloudera.manager.advanced.service.discovery.config.monitor.interval

Default Value

10 second(s)

API Name

gateway_auto_discovery_advanced_configuration_monitor_interval

Required

false

Enable Auto Discovery (cdp-proxy-api) - Atlas API

Description

Enables Knox auto-discovery for the Atlas API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.atlas-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_atlas

Required

false

Enable Auto Discovery (cdp-proxy-api) - Phoenix/Avatica

Description

Enables Knox auto-discovery for the Phoenix/Avatica API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.avatica

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_avatica

Required

false

Enable Auto Discovery (cdp-proxy-api) - Cloudera Manager API

Description

Enables Knox auto-discovery for the Cloudera Manager API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.cm-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_cm_api

Required

false

Enable Auto Discovery (cdp-proxy-api) - Cruise Control API

Description

Enables Knox auto-discovery for the Cruise Control API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.cruise-control-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_cruise_control

Required

false

Enable Auto Discovery (cdp-proxy-api) - Hive Server

Description

Enables Knox auto-discovery for the Hive Server in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.hive

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_hive

Required

false

Enable Auto Discovery (cdp-proxy-api) - Impala Catalog Server

Description

Enables Knox auto-discovery for the Impala Catalog Server in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.impala

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_impala

Required

false

Enable Auto Discovery (cdp-proxy-api) - Livy Server For Spark3 API

Description

Enables Knox auto-discovery for the Livy Server For Spark3 API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.livy_for_spark3

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_livy_for_spark3

Required

false

Enable Auto Discovery (cdp-proxy-api) - Livy Server API

Description

Enables Knox auto-discovery for the Livy Server API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.livyserver

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_livyserver

Required

false

Enable Auto Discovery (cdp-proxy-api) - NameNode

Description

Enables Knox auto-discovery for the NameNode in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.namenode

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_namenode

Required

false

Enable Auto Discovery (cdp-proxy-api) - NiFi

Description

Enables Knox auto-discovery for the NiFi in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.nifi

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_nifi

Required

false

Enable Auto Discovery (cdp-proxy-api) - NiFi Registry

Description

Enables Knox auto-discovery for the NiFi Registry in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.nifi-registry

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_nifi_registry

Required

false

Enable Auto Discovery (cdp-proxy-api) - Oozie Server

Description

Enables Knox auto-discovery for the Oozie Server in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.oozie

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_oozie

Required

false

Enable Auto Discovery (cdp-proxy-api) - Profiler Admin API

Description

Enables Knox auto-discovery for the Profiler Admin API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.profiler-admin-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_profiler_admin_api

Required

false

Enable Auto Discovery (cdp-proxy-api) - Profiler Metrics API

Description

Enables Knox auto-discovery for the Profiler Metrics API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.profiler-metrics-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_profiler_metrics_api

Required

false

Enable Auto Discovery (cdp-proxy-api) - Profiler Scheduler API

Description

Enables Knox auto-discovery for the Profiler Scheduler API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.profiler-scheduler-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_profiler_scheduler_api

Required

false

Enable Auto Discovery (cdp-proxy-api) - Ranger Admin

Description

Enables Knox auto-discovery for the Ranger Admin in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.ranger

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_ranger

Required

false

Enable Auto Discovery (cdp-proxy-api) - ResourceManager

Description

Enables Knox auto-discovery for the ResourceManager in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.resourcemanager

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_resourcemanager

Required

false

Enable Auto Discovery (cdp-proxy-api) - ResourceManager API

Description

Enables Knox auto-discovery for the ResourceManager API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.resourcemanagerapi

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_resourcemanager_api

Required

false

Enable Auto Discovery (cdp-proxy-api) - Schema Registry

Description

Enables Knox auto-discovery for the Schema Registry in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.schema-registry

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_schema_registry

Required

false

Enable Auto Discovery (cdp-proxy-api) - Stream Messaging Manager API

Description

Enables Knox auto-discovery for the Stream Messaging Manager API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.smm-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_smm

Required

false

Enable Auto Discovery (cdp-proxy-api) - Solr Server

Description

Enables Knox auto-discovery for the Solr Server in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.solr

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_solr

Required

false

Enable Auto Discovery (cdp-proxy-api) - HBase Master API

Description

Enables Knox auto-discovery for the HBase Master API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.webhbase

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_webhbase

Required

false

Enable Auto Discovery (cdp-proxy-api) - WebHDFS API

Description

Enables Knox auto-discovery for the WebHDFS API in the cdp-proxy-api topology.

Related Name

gateway.auto.discovery.cdp-proxy-api.enabled.webhdfs

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_api_enabled_webhdfs

Required

false

Enable Auto Discovery (cdp-proxy) - Atlas API

Description

Enables Knox auto-discovery for the Atlas API in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.atlas-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_atlas

Required

false

Enable Auto Discovery (cdp-proxy) - Atlas Web UI

Description

Enables Knox auto-discovery for the Atlas Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.atlas

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_atlas_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Cloudera Manager API

Description

Enables Knox auto-discovery for the Cloudera Manager API in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.cm-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_cm_api

Required

false

Enable Auto Discovery (cdp-proxy) - Cloudera Manager Admin Console

Description

Enables Knox auto-discovery for the Cloudera Manager Admin Console in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.cm-ui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_cm_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Data Analytics Studio

Description

Enables Knox auto-discovery for the Data Analytics Studio in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.das

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_das

Required

false

Enable Auto Discovery (cdp-proxy) - Flink Dashboard

Description

Enables Knox auto-discovery for the Flink Dashboard in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.flink-dashboard

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_flink_dashboard

Required

false

Enable Auto Discovery (cdp-proxy) - HBase Web UI

Description

Enables Knox auto-discovery for the HBase Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.hbaseui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_hbase_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Namenode Web UI

Description

Enables Knox auto-discovery for the Namenode Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.hdfsui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_hdfs_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Hue Server

Description

Enables Knox auto-discovery for the Hue Server in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.hue

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_hue

Required

false

Enable Auto Discovery (cdp-proxy) - Impala Catalog Server Web UI

Description

Enables Knox auto-discovery for the Impala Catalog Server Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.impalaui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_impala_ui

Required

false

Enable Auto Discovery (cdp-proxy) - HistoryServer Web UI

Description

Enables Knox auto-discovery for the HistoryServer Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.jobhistoryui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_jobhistory_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Kudu Master Web UI

Description

Enables Knox auto-discovery for the Kudu Master Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.kuduui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_kudu_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Livy Server For Spark3 Web UI

Description

Enables Knox auto-discovery for the Livy Server For Spark3 Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.livy_for_spark3

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_livy_for_spark3

Required

false

Enable Auto Discovery (cdp-proxy) - Livy Server Web UI

Description

Enables Knox auto-discovery for the Livy Server Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.livyserver

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_livyserver

Required

false

Enable Auto Discovery (cdp-proxy) - NameNode

Description

Enables Knox auto-discovery for the NameNode in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.namenode

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_namenode

Required

false

Enable Auto Discovery (cdp-proxy) - NiFi

Description

Enables Knox auto-discovery for the NiFi in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.nifi

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_nifi

Required

false

Enable Auto Discovery (cdp-proxy) - NiFi Registry

Description

Enables Knox auto-discovery for the NiFi Registry in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.nifi-registry

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_nifi_registry

Required

false

Enable Auto Discovery (cdp-proxy) - Oozie Server

Description

Enables Knox auto-discovery for the Oozie Server in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.oozie

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_oozie

Required

false

Enable Auto Discovery (cdp-proxy) - Oozie Web UI

Description

Enables Knox auto-discovery for the Oozie Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.oozieui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_oozie_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Ranger Admin

Description

Enables Knox auto-discovery for the Ranger Admin in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.ranger

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_ranger

Required

false

Enable Auto Discovery (cdp-proxy) - Ranger Admin Web UI

Description

Enables Knox auto-discovery for the Ranger Admin Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.rangerui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_ranger_ui

Required

false

Enable Auto Discovery (cdp-proxy) - ResourceManager

Description

Enables Knox auto-discovery for the ResourceManager in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.resourcemanager

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_resourcemanager

Required

false

Enable Auto Discovery (cdp-proxy) - Schema Registry

Description

Enables Knox auto-discovery for the Schema Registry in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.schema-registry

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_schema_registry

Required

false

Enable Auto Discovery (cdp-proxy) - Stream Messaging Manager API

Description

Enables Knox auto-discovery for the Stream Messaging Manager API in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.smm-api

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_smm

Required

false

Enable Auto Discovery (cdp-proxy) - Stream Messaging Manager Web UI

Description

Enables Knox auto-discovery for the Stream Messaging Manager Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.smm-ui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_smm_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Solr Server

Description

Enables Knox auto-discovery for the Solr Server in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.solr

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_solr

Required

false

Enable Auto Discovery (cdp-proxy) - Spark 3 History Server Web UI

Description

Enables Knox auto-discovery for the Spark 3 History Server Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.spark3historyui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_spark3history_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Spark History Server Web UI

Description

Enables Knox auto-discovery for the Spark History Server Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.sparkhistoryui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_sparkhistory_ui

Required

false

Enable Auto Discovery (cdp-proxy) - WebHDFS API

Description

Enables Knox auto-discovery for the WebHDFS API in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.webhdfs

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_webhdfs

Required

false

Enable Auto Discovery (cdp-proxy) - ResourceManager Web UI

Description

Enables Knox auto-discovery for the ResourceManager Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.yarnui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_yarn_ui

Required

false

Enable Auto Discovery (cdp-proxy) - ResourceManager Web UI V2

Description

Enables Knox auto-discovery for the ResourceManager Web UI V2 in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.yarnuiv2

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_yarn_ui_v2

Required

false

Enable Auto Discovery (cdp-proxy) - Zeppelin Server Web UI

Description

Enables Knox auto-discovery for the Zeppelin Server Web UI in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.zeppelinui

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_zeppelin_ui

Required

false

Enable Auto Discovery (cdp-proxy) - Zeppelin Server

Description

Enables Knox auto-discovery for the Zeppelin Server in the cdp-proxy topology.

Related Name

gateway.auto.discovery.cdp-proxy.enabled.zeppelinws

Default Value

true

API Name

gateway_auto_discovery_cdp_proxy_enabled_zeppelin_ws

Required

false

Enable/Disable Service Auto-Discovery

Description

Whether Knox's service auto-discovery feature is enabled

Related Name

gateway.auto.discovery.enabled

Default Value

true

API Name

gateway_auto_discovery_enabled

Required

false

Knox Simplified Topology Management - Monitoring Interval

Description

Defines the frequency of Cloudera Manager resources (descriptors and shared providers) file (cdp-resources.xml) monitoring.

Related Name

gateway.cloudera.manager.descriptors.monitor.interval

Default Value

10 second(s)

API Name

gateway_cloudera_manager_descriptors_monitor_interval

Required

false

Auto Discovery - Cluster Configuration Monitoring Interval

Description

Defines the frequency of cluster configuration monitoring.

Related Name

gateway.cluster.config.monitor.cm.interval

Default Value

1 minute(s)

API Name

gateway_cluster_configuration_monitor_interval

Required

false

Knox Gateway Configuration Directory

Description

Contains configuration files that apply to the gateway globally (i.e. not cluster specific).

Related Name

gateway_conf_dir

Default Value

/var/lib/knox/gateway/conf

API Name

gateway_conf_dir

Required

false

Knox Gateway Data Directory

Description

Contains security and topology specific artifacts as well as important applications for admin-ui

Related Name

gateway_data_dir

Default Value

/var/lib/knox/gateway/data

API Name

gateway_data_dir

Required

false

Gateway - Default App Topology Name

Description

When a topology file is deployed with a file name that matches the configured default topology name, a specialized mapping for URLs is installed for that particular topology. This allows the URLs that are expected by the existing Hadoop CLIs for WebHDFS to be used in interacting with the specific Hadoop cluster that is represented by the default topology file.

Related Name

default.app.topology.name

Default Value

cdp-proxy

API Name

gateway_default_topology_name

Required

false

Knox Simplified Topology Management - cdp-proxy

Description

Knox descriptor block for 'cdp-proxy' topology. 'providerConfigRef' indicates the name of shared-provider the given descriptor would like to use. The rest of the entries hold service information. The structure of an service information entry is: $SERVICE_NAME[:$PARAMETER_NAME=$PARAMETER_VALUE]. The 'url' and 'version' parameter names are preserved keywords to set the given service's URL and version. For instance: HIVE:url=http://localhost:123, HIVE:version:3.0.0, HIVE:httpclient.socketTimeout=5m, HIVE:test.pramameter.name=test.parameter.value

Related Name

cdp-proxy

Default Value

providerConfigRef=sso

API Name

gateway_descriptor_cdp_proxy

Required

false

Knox Simplified Topology Management - cdp-proxy-api

Description

Knox descriptor block for 'cdp-proxy-api topology. 'providerConfigRef' indicates the name of shared-provider the given descriptor would like to use. The rest of the entries hold service information. The structure of an service information entry is: $SERVICE_NAME[:$PARAMETER_NAME=$PARAMETER_VALUE]. The 'url' and 'version' parameter names are preserved keywords to set the given service's URL and version. For instance: NIFI, HIVE:url=http://localhost:123, HIVE:version:3.0.0, HIVE:httpclient.socketTimeout=5m, HIVE:test.pramameter.name=test.parameter.value

Related Name

cdp-proxy-api

Default Value

providerConfigRef=pam

API Name

gateway_descriptor_cdp_proxy_api

Required

false

Knox Gateway Dispatch Whitelist

Description

The whitelist to be applied for dispatches associated with the service roles specified by gateway.dispatch.whitelist.services. By default this is replaced with DEFAULT or HTTPS_ONLY based on if TLS is enabled.

Related Name

gateway.dispatch.whitelist

Default Value

WHITELIST_CONFIG_REPLACEME

API Name

gateway_dispatch_whitelist

Required

false

Knox Gateway Dispatch Whitelist Services

Description

The comma-delimited list of service roles for which the 'gateway.dispatch.whitelist' should be applied

Related Name

gateway.dispatch.whitelist.services

Default Value

DATANODE, HBASEUI, HDFSUI, IMPALAUI, JOBHISTORYUI, KUDUUI, NODEUI, YARNUI, YARNUIV2, knoxauth

API Name

gateway_dispatch_whitelist_services

Required

false

Gateway Config Directory

Description

The directory within 'gateway_data_dir' that contains gateway topology files and deployments.

Related Name

gateway.gateway.conf.dir

Default Value

deployments

API Name

gateway_gateway_conf_dir

Required

false

Knox Gateway Initial/Max Heapsize

Description

Initial/Maximum size for the Java Process heap. Passed to Java -Xmx/-Xms. Measured in megabytes.

Related Name

gateway_heap_size

Default Value

1 GiB

API Name

gateway_heap_size

Required

true

Additional Gateway Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags are passed here. -Xmx/-Xms should not be specified here: to set the heapsize use the 'Knox Gateway Initial/Max Heapsize' parameter

Related Name

gateway_java_opts

Default Value

API Name

gateway_java_opts

Required

false

Admin Groups

Description

Admin groups for Knox

Related Name

gateway.knox.admin.groups

Default Value

API Name

gateway_knox_admin_groups

Required

false

Knox Master Secret

Description

The master secret is used to access secured artifacts by the gateway instance. Keystore, trust stores and credential stores are all protected with the master secret. NOTE: changing the master secret will require you to change passwords protecting the keystores for the gateway, identity keystores and all credential stores

Related Name

gateway_master_secret

Default Value

API Name

gateway_master_secret

Required

true

Gateway Path

Description

The default context path for the gateway.

Related Name

gateway.path

Default Value

gateway

API Name

gateway_path

Required

true

Ranger Knox Plugin Conf Path

Description

Staging directory for Ranger Knox Plugin Configuration. This should generally not be changed.

Related Name

gateway_ranger_knox_plugin_conf_path

Default Value

/var/lib/knox/ranger-knox-plugin

API Name

gateway_ranger_knox_plugin_conf_path

Required

true

Ranger Knox Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/knox/gateway/audit/hdfs/spool

API Name

gateway_ranger_knox_plugin_hdfs_audit_spool_directory

Required

true

Ranger Knox Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.knox.policy.cache.dir

Default Value

/var/lib/ranger/knox/gateway/policy-cache

API Name

gateway_ranger_knox_plugin_policy_cache_directory

Required

true

Ranger Knox Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/knox/gateway/audit/solr/spool

API Name

gateway_ranger_knox_plugin_solr_audit_spool_directory

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.knox.trusted.proxy.ipaddress

Default Value

API Name

gateway_ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.knox.use.x-forwarded-for.ipaddress

Default Value

false

API Name

gateway_ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Cookie Scoping Enabled

Description

Enable/Disable cookie scoping feature.

Related Name

gateway.scope.cookies.feature.enabled

Default Value

false

API Name

gateway_scope_cookies_feature_enabled

Required

false

Security - Signing Key Alias

Description

The alias for the signing keypair within the keystore specified via gateway_signing_keystore_name

Related Name

gateway.signing.key.alias

Default Value

API Name

gateway_signing_key_alias

Required

false

Security - Signing Keystore Name

Description

The filename of keystore file that contains the signing keypair

Related Name

gateway.signing.keystore.name

Default Value

API Name

gateway_signing_keystore_name

Required

false

Security - Signing Keystore Type

Description

The type of the keystore file where the signing keypair is stored. See gateway_signing_keystore_name

Related Name

gateway.signing.keystore.type

Default Value

API Name

gateway_signing_keystore_type

Required

false

Knox Simplified Topology Management - SSO Authentication Provider

Description

Authentication provider declaration used by the UIs using the Knox SSO capabilities such as the Admin and Home Page UIs.

Related Name

gateway_sso_authentication_provider

Default Value

role=authentication authentication.name=ShiroProvider authentication.param.sessionTimeout=30 authentication.param.redirectToUrl=/$GATEWAY_PATH/knoxsso/knoxauth/login.html authentication.param.restrictedCookies=rememberme, WWW-Authenticate authentication.param.main.pamRealm=org.apache.knox.gateway.shirorealm.KnoxPamRealm authentication.param.main.pamRealm.service=login authentication.param.urls./**=authcBasic

API Name

gateway_sso_authentication_provider

Required

false

Security - TLS Certificate Alias (Optional)

Description

The alias for the Gateway's TLS certificate and keypair within the default keystore or the keystore specified via gateway.tls.keystore.path

Related Name

gateway_tls_certificate_alias

Default Value

API Name

gateway_tls_certificate_alias

Required

false

Security - Use FQDN as TLS Certificate Alias

Description

If enabled, the FQDN will be used as gateway.tls.key.alias in gateway-site.xml; otherwise the UQDN is used. This behavior is overwritten if gateway_tls_certificate_alias is set. In this case the value in gateway_tls_certificate_alias is used as alias.

Related Name

gateway_tls_certificate_alias_use_fqdn

Default Value

true

API Name

gateway_tls_certificate_alias_use_fqdn

Required

false

Security - TLS Certificate Path (Optional)

Description

The path for the TLS certificate which Knox will import in the CM generated/distributed keystore in case SSL is enabled (if any).

Related Name

gateway_tls_certificate_path

Default Value

API Name

gateway_tls_certificate_path

Required

false

Websockets Enabled

Description

Enable/Disable websocket feature.

Related Name

gateway.websocket.feature.enabled

Default Value

true

API Name

gateway_websocket_feature_enabled

Required

false

X-Forwarded Header Context Service Name

Description

The service name to be added in x-forward-context header.

Related Name

gateway.xforwarded.header.context.append.servicename

Default Value

LIVYSERVER, LIVY_FOR_SPARK3

API Name

gateway_xforwarded_header_context_append_servicename

Required

false

Admin Group Mapping - Class Name

Description

The class name used for Hadoop admin group mapping

Related Name

gateway.group.config.hadoop.security.group.mapping

Default Value

org.apache.hadoop.security.ShellBasedUnixGroupsMapping

API Name

hadoop_security_group_mapping_class

Required

false

Hadoop Group Mapping - Negative Cache Expiration

Description

The Hadoop group mapping negative cache expiration in seconds

Related Name

gateway.group.config.hadoop.security.groups.negative-cache.secs

Default Value

5 second(s)

API Name

hadoop_security_group_negative_cache_expiration_seconds

Required

false

Hadoop Group Mapping - Positive Cache Expiration

Description

The Hadoop group mapping positive cache expiration in seconds

Related Name

gateway.group.config.hadoop.security.groups.cache.secs

Default Value

10 second(s)

API Name

hadoop_security_group_positive_cache_expiration_seconds

Required

false

krb5.conf Location

Description

Absolute path to krb5.conf file

Related Name

java.security.krb5.conf

Default Value

/etc/krb5.conf

API Name

java_security_krb5_conf

Required

false

KRB5 Debug

Description

Boolean flag indicating whether to enable debug messages for krb5 authentication

Related Name

sun.security.krb5.debug

Default Value

false

API Name

sun_security_krb5_debug

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Gateway HTTP Port

Description

The HTTP port for the Gateway.

Related Name

gateway.port

Default Value

8443

API Name

gateway_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Knox Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Knox Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

gateway.httpclient.truststore.path

Default Value

API Name

ssl_client_truststore_location

Required

false

Knox Gateway TLS/SSL Trust Store Password

Description

The password for the Knox Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Knox Gateway

Description

Encrypt communication between clients and Knox Gateway using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

knox.enableTLS

Default Value

false

API Name

ssl_enabled

Required

false

Knox Gateway TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Knox Gateway is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

gateway.tls.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

Knox Gateway TLS/SSL Server Keystore File Password

Description

The password for the Knox Gateway keystore file.

Related Name

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/auto-discovery-advanced-configuration-cdp-proxy.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/cdp-resources.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/cdp-resources.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/cdp-resources.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/gateway-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox Simplified Topology Management - API Authentication Provider

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Simplified Topology Management - API Authentication Provider parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_api_authentication_provider

Required

true

Suppress Parameter Validation: Knox Gateway Configuration Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Configuration Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_conf_dir

Required

true

Suppress Parameter Validation: Knox Gateway Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_data_dir

Required

true

Suppress Parameter Validation: Gateway - Default App Topology Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway - Default App Topology Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_default_topology_name

Required

true

Suppress Parameter Validation: Knox Simplified Topology Management - cdp-proxy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Simplified Topology Management - cdp-proxy parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_descriptor_cdp_proxy

Required

true

Suppress Parameter Validation: Knox Simplified Topology Management - cdp-proxy-api

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Simplified Topology Management - cdp-proxy-api parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_descriptor_cdp_proxy_api

Required

true

Suppress Parameter Validation: Knox Gateway Dispatch Whitelist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Dispatch Whitelist parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_dispatch_whitelist

Required

true

Suppress Parameter Validation: Knox Gateway Dispatch Whitelist Services

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Dispatch Whitelist Services parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_dispatch_whitelist_services

Required

true

Suppress Parameter Validation: Gateway Config Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Config Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_gateway_conf_dir

Required

true

Suppress Parameter Validation: Knox Gateway Initial/Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Initial/Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_heap_size

Required

true

Suppress Parameter Validation: Additional Gateway Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Gateway Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_java_opts

Required

true

Suppress Parameter Validation: Admin Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_knox_admin_groups

Required

true

Suppress Parameter Validation: Knox Master Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Master Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_master_secret

Required

true

Suppress Parameter Validation: Gateway Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_path

Required

true

Suppress Parameter Validation: Gateway HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_port

Required

true

Suppress Parameter Validation: Ranger Knox Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Knox Plugin Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_conf_path

Required

true

Suppress Parameter Validation: Ranger Knox Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Knox Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Knox Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Knox Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Knox Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Knox Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Security - Signing Key Alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Key Alias parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_key_alias

Required

true

Suppress Parameter Validation: Security - Signing Keystore Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Keystore Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_keystore_name

Required

true

Suppress Parameter Validation: Security - Signing Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_keystore_type

Required

true

Suppress Parameter Validation: Knox Simplified Topology Management - SSO Authentication Provider

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Simplified Topology Management - SSO Authentication Provider parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_sso_authentication_provider

Required

true

Suppress Parameter Validation: Security - TLS Certificate Alias (Optional)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - TLS Certificate Alias (Optional) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_tls_certificate_alias

Required

true

Suppress Parameter Validation: Security - TLS Certificate Path (Optional)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - TLS Certificate Path (Optional) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_tls_certificate_path

Required

true

Suppress Parameter Validation: X-Forwarded Header Context Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the X-Forwarded Header Context Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_xforwarded_header_context_append_servicename

Required

true

Suppress Parameter Validation: Admin Group Mapping - Class Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Group Mapping - Class Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_group_mapping_class

Required

true

Suppress Parameter Validation: krb5.conf Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the krb5.conf Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_java_security_krb5_conf

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Knox Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_knox_gateway_role_env_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Knox Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Knox Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Knox Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Knox Gateway TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Knox Gateway TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Gateway TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_knox_gateway_unexpected_exits

Required

true

Knox IDBroker

Advanced

Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-reloadable.xml

Description

For advanced use only. A string to be inserted into conf/gateway-reloadable.xml for this role only.

Related Name

Default Value

API Name

conf/gateway-reloadable.xml_role_safety_valve

Required

false

Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

For advanced use only. A string to be inserted into conf/gateway-site.xml for this role only.

Related Name

Default Value

API Name

conf/gateway-site.xml_role_safety_valve

Required

false

Knox IDBroker Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

IDBROKER_role_env_safety_valve

Required

false

Knox IDBroker Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value
20

API Name
process_start_secs

Required
false

Logs

Knox IDBroker Log Directory

Description
The log directory for log files of the role Knox IDBroker.

Related Name
log_dir

Default Value
/var/log/knox/idbroker

API Name
log_dir

Required
false

Knox IDBroker Logging Threshold

Description
The minimum log level for Knox IDBroker logs

Related Name

Default Value
INFO

API Name
log_threshold

Required
false

Knox IDBroker Maximum Log File Backups

Description
The maximum number of rolled log files to keep for Knox IDBroker logs. Typically used by log4j or logback.

Related Name

Default Value
10

API Name
max_log_backup_index

Required
false

Knox IDBroker Max Log Size

Description

The maximum size, in megabytes, per log file for Knox IDBroker logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

idbroker_fd_thresholds

Required

false

Knox IDBroker Host Health Test

Description

When computing the overall Knox IDBroker health, consider the host's health.

Related Name

Default Value

true

API Name

idbroker_host_health_enabled

Required

false

Knox IDBroker Process Health Test

Description

Enables the health test that the Knox IDBroker's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

idbroker_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Knox IDBroker Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Knox IDBroker AWS Credentials Key

Description

The AWS credentials key

Related Name

idbroker_aws_credentials_key

Default Value

API Name

idbroker_aws_credentials_key

Required

false

Knox IDBroker AWS Credentials Secret

Description

The AWS credentials secret

Related Name

idbroker_aws_credentials_secret

Default Value

API Name

idbroker_aws_credentials_secret

Required

false

Knox IDBroker AWS Group Mapping

Description

The list of AWS group-role mappings in 'group=role[;group=role]...[;group=role]' format. A 'group=role' declaration indicates that all authenticated users that are member of the specified group should be able to assume the specified role. For instance: admin=arn:aws:iam:XYZ:role/s3full;audit=arn:aws:iam:XYZ:role/s3Read

Related Name

idbroker.aws.group.role.mapping

Default Value

API Name

idbroker_aws_group_mapping

Required

false

Knox IDBroker AWS User Default Group Mapping

Description

The list of AWS user default group mappings in 'user=group[;user=group;...;user=group]' format. A 'user=group' declaration allows the given user to get its credentials indicated by the given group (in case the user belongs to different mapped groups)

Related Name

idbroker.aws.user.default.group.mapping

Default Value

API Name

idbroker_aws_user_default_group_mapping

Required

false

Knox IDBroker AWS User Mapping

Description

The list of AWS user-role mappings in 'user=role[;user=role]...[;user=role]' format. A 'user=role' declaration indicates that this is a mapping of the authenticated user’s primary principal to the specified role. For instance: admin=arn:aws:iam:XYZ:role/s3full;guest=arn:aws:iam:XYZ:role/s3Read

Related Name

idbroker.aws.user.role.mapping

Default Value

API Name

idbroker_aws_user_mapping

Required

false

Knox IDBroker AZURE ADLS2 Tenant Name

Description

The name of the AZURE AD tenant. A tenant is a representation of an organization. It's a dedicated instance of Azure AD that an organization or application developer receives when the organization or application developer creates a relationship with Microsoft

Related Name

idbroker_azure_adls2_tenant_name

Default Value

API Name

idbroker_azure_adls2_tenant_name

Required

false

Knox IDBroker AZURE 'blob-contributor' ClientID

Description

The client ID credential for 'blob-contributor' role

Related Name

idbroker_azure_blob_contributor_clientid

Default Value

API Name

idbroker_azure_blob_contributor_clientid

Required

false

Knox IDBroker AZURE 'blob-contributor' Secret

Description

The secret credential for 'blob-contributor' role

Related Name

idbroker_azure_blob_contributor_secret

Default Value

API Name

idbroker_azure_blob_contributor_secret

Required

false

Knox IDBroker AZURE 'blob-reader' ClientID

Description

The client ID credential for 'blob-reader' role

Related Name

idbroker_azure_blob_reader_clientid

Default Value

API Name

idbroker_azure_blob_reader_clientid

Required

false

Knox IDBroker AZURE 'blob-reader' Secret

Description

The secret credential for 'blob-reader' role

Related Name

idbroker_azure_blob_reader_secret

Default Value

API Name

idbroker_azure_blob_reader_secret

Required

false

Knox IDBroker AZURE Group Mapping

Description

The list of AZURE group-role mappings in 'group=role[;group=role]...[;group=role]' format. A 'group=role' declaration indicates that all authenticated users that are member of the specified group should be able to assume the specified role. For instance: admin=blob-contributor

Related Name

idbroker.adls2.group.role.mapping

Default Value

API Name

idbroker_azure_group_mapping

Required

false

Knox IDBroker AZURE User Default Group Mapping

Description

The list of AZURE user default group mappings in 'user=group[;user=group;...;user=group]' format. A 'user=group' declaration allows the given user to get its credentials indicated by the given group (in case the user belongs to different mapped groups)

Related Name

idbroker.azure.user.default.group.mapping

Default Value

API Name

idbroker_azure_user_default_group_mapping

Required

false

Knox IDBroker AZURE User Mapping

Description

The list of AZURE user-role mappings in 'user=role[;user=role]...[;user=role]' format. A 'user=role' declaration indicates that this is a mapping of the authenticated user’s primary principal to the specified role. For instance: admin=blob-contributor

Related Name

idbroker.adls2.user.role.mapping

Default Value

API Name

idbroker_azure_user_mapping

Required

false

Knox IDBroker AZURE VM Assumer Identity

Description

A user assigned managed identity that has Virtual Machine Contributor and Managed Identity Operator roles scoped at the resource group where IDBroker Virtual Machine is running.

Related Name

idbroker_azure_vm_assumer_identity

Default Value

API Name

idbroker_azure_vm_assumer_identity

Required

false

Knox IDBroker Configuration Directory

Description

Contains configuration files that apply to the gateway globally (i.e. not cluster specific).

Related Name

idbroker_conf_dir

Default Value

/var/lib/knox/idbroker/conf

API Name

idbroker_conf_dir

Required

false

Knox IDBroker Data Directory

Description

Contains security and topology specific artifacts as well as important applications for admin-ui

Related Name

idbroker_data_dir

Default Value

/var/lib/knox/idbroker/data

API Name

idbroker_data_dir

Required

false

Gateway - Default App Topology Name

Description

When a topology file is deployed with a file name that matches the configured default topology name, a specialized mapping for URLs is installed for that particular topology. This allows the URLs that are expected by the existing Hadoop CLIs for WebHDFS to be used in interacting with the specific Hadoop cluster that is represented by the default topology file.

Related Name

default.app.topology.name

Default Value

API Name

idbroker_default_topology_name

Required

false

Gateway Config Directory

Description

The directory within 'idbroker_data_dir' that contains gateway topology files and deployments.

Related Name

gateway.gateway.conf.dir

Default Value

deployments

API Name

idbroker_gateway_gateway_conf_dir

Required

false

Admin Groups

Description

Admin groups for Knox

Related Name

gateway.knox.admin.groups

Default Value

API Name

idbroker_gateway_knox_admin_groups

Required

false

Gateway Path

Description

The default context path for the gateway.

Related Name

gateway.path

Default Value

gateway

API Name

idbroker_gateway_path

Required

true

Cookie Scoping Enabled

Description

Enable/Disable cookie scoping feature.

Related Name

gateway.scope.cookies.feature.enabled

Default Value

false

API Name

idbroker_gateway_scope_cookies_feature_enabled

Required

false

Security - Signing Key Alias

Description

The alias for the signing keypair within the keystore specified via idbroker_gateway_signing_keystore_name

Related Name

gateway.signing.key.alias

Default Value

API Name

idbroker_gateway_signing_key_alias

Required

false

Security - Signing Keystore Name

Description

The filename of keystore file that contains the signing keypair

Related Name

gateway.signing.keystore.name

Default Value

API Name

idbroker_gateway_signing_keystore_name

Required

false

Security - Signing Keystore Type

Description

The type of the keystore file where the signing keypair is stored. See idbroker_gateway_signing_keystore_name

Related Name

gateway.signing.keystore.type

Default Value

API Name

idbroker_gateway_signing_keystore_type

Required

false

Knox IDBroker GCP Credential Key

Description

The GCP Credential Key

Related Name

idbroker_gcp_credential_key

Default Value

API Name

idbroker_gcp_credential_key

Required

false

Knox IDBroker GCP Credential Secret

Description

The GCP Credential Secret

Related Name

idbroker_gcp_credential_secret

Default Value

API Name

idbroker_gcp_credential_secret

Required

false

Knox IDBroker GCP Group Mapping

Description

The list of GCP group-role mappings in 'group=role[;group=role]...[;group=role]' format. A 'group=role' declaration indicates that all authenticated users that are member of the specified group should be able to assume the specified role. For instance: admin=storage-admin@XYZ.iam.gserviceaccount.com;audit=storage-read-only@XYZ.iam.gserviceaccount.com

Related Name

idbroker.gcp.group.role.mapping

Default Value

API Name

idbroker_gcp_group_mapping

Required

false

Knox IDBroker GCP User Default Group Mapping

Description

The list of GCP user default group mappings in 'user=group[;user=group;...;user=group]' format. A 'user=group' declaration allows the given user to get its credentials indicated by the given group (in case the user belongs to different mapped groups)

Related Name

idbroker.gcp.user.default.group.mapping

Default Value

API Name

idbroker_gcp_user_default_group_mapping

Required

false

Knox IDBroker GCP User Mapping

Description

The list of GCP user-role mappings in 'user=role[;user=role]...[;user=role]' format. A 'user=role' declaration indicates that this is a mapping of the authenticated user's primary principal to the specified role. For instance: admin=storage-admin@XYZ.iam.gserviceaccount.com;guest=storage-read-only@XYZ.iam.gserviceaccount.com

Related Name

idbroker.gcp.user.role.mapping

Default Value

API Name

idbroker_gcp_user_mapping

Required

false

Admin Group Mapping - Class Name

Description

The class name used for Hadoop admin group mapping

Related Name

gateway.group.config.hadoop.security.group.mapping

Default Value

org.apache.hadoop.security.ShellBasedUnixGroupsMapping

API Name

idbroker_hadoop_security_group_mapping_class

Required

false

IDBroker Initial/Max Heapsize

Description

Initial/Maximum size for the Java Process heap. Passed to Java -Xmx/-Xms. Measured in megabytes.

Related Name

idbroker_heap_size

Default Value

1 GiB

API Name

idbroker_heap_size

Required

true

Additional IDBroker Java Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags are passed here. -Xmx/-Xms should not be specified here: to set the heapsize use the 'Knox Gateway Initial/Max Heapsize' parameter

Related Name

idbroker_java_opts

Default Value

API Name

idbroker_java_opts

Required

false

krb5.conf Location

Description

Absolute path to krb5.conf file

Related Name

java.security.krb5.conf

Default Value

/etc/krb5.conf

API Name

idbroker_java_security_krb5_conf

Required

false

Kerberos Proxyuser Block

Description

Proxyuser configuration used in Knox's 'dt' topology in case Kerberos is enabled. Must conform a valid JSON key-value format!

Related Name

idbroker_kerberos_dt_proxyuser_block

Default Value

hadoop.proxyuser.livy.hosts: * hadoop.proxyuser.livy.groups: * hadoop.proxyuser.hive.hosts: * hadoop.proxyuser.hive.groups: * hadoop.proxyuser.httpfs.hosts: * hadoop.proxyuser.httpfs.groups: * hadoop.proxyuser.hue.hosts: * hadoop.proxyuser.hue.groups: * hadoop.proxyuser.oozie.hosts: * hadoop.proxyuser.oozie.groups: * hadoop.proxyuser.impala.hosts: * hadoop.proxyuser.impala.groups: *

API Name

idbroker_kerberos_dt_proxyuser_block

Required

false

IDBroker Knox Token Eviction Grace Period

Description

Defines the grace period for which an expired token's state will avoid eviction. Setting this to zero means there is no grace period, and token state is evicted based on expiration only. See idbroker_knox_token_eviction_interval for more information.

Related Name

gateway.knox.token.eviction.grace.period

Default Value

1 day(s)

API Name

idbroker_knox_token_eviction_grace_period

Required

false

IDBroker Knox Token Eviction Interval

Description

Defines the interval on which Knox will check for expired token state which should be evicted. If the value is equal to zero, Knox will not perform this check.

Related Name

gateway.knox.token.eviction.interval

Default Value

1 minute(s)

API Name

idbroker_knox_token_eviction_interval

Required

false

IDBroker Knox Token Permissive Validation

Description

When enabled, Knox will verify tokens for which there is no server-managed state based only on the contents of the tokens themselves, rather than throwing UnknownToken exceptions.

Related Name

gateway.knox.token.permissive.validation

Default Value

false

API Name

idbroker_knox_token_permissive_validation

Required

false

Enable IDBroker Knox Token State Server

Description

Whether the Knox token state server is enabled for IDBroker

Related Name

idbroker_knox_token_state_enabled

Default Value

false

API Name

idbroker_knox_token_state_enabled

Required

false

IDBroker Knox Token TTL

Description

This indicates the lifespan of the token. Once it expires a new token must be acquired from KnoxToken service. This is in milliseconds.

Related Name

idbroker_knox_token_ttl_ms

Default Value

7 day(s)

API Name

idbroker_knox_token_ttl_ms

Required

false

IDBroker Master Secret

Description

The master secret is used to access secured artifacts by the gateway instance. Keystore, trust stores and credential stores are all protected with the master secret. NOTE: changing the master secret will require you to change passwords protecting the keystores for the gateway, identity keystores and all credential stores

Related Name

idbroker_master_secret

Default Value

API Name

idbroker_master_secret

Required

true

Gateway Config Refresh Interval

Description

Defines the frequency of gateway configuration refresh.

Related Name

gateway.config.refresh.interval

Default Value

10 second(s)

API Name

idbroker_relaodable_refresh_interval_ms

Required

false

KRB5 Debug

Description

Boolean flag indicating whether to enable debug messages for krb5 authentication

Related Name

sun.security.krb5.debug

Default Value

false

API Name

idbroker_sun_security_krb5_debug

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Gateway HTTP Port

Description

The HTTP port for the Gateway.

Related Name

gateway.port

Default Value

8444

API Name

idbroker_gateway_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Knox IDBroker TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Knox IDBroker might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

gateway.httpclient.truststore.path

Default Value

API Name

ssl_client_truststore_location

Required

false

Knox IDBroker TLS/SSL Trust Store Password

Description

The password for the Knox IDBroker TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Knox IDBroker

Description

Encrypt communication between clients and Knox IDBroker using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

knox.enableTLS

Default Value

false

API Name

ssl_enabled

Required

false

Knox IDBroker TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Knox IDBroker is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

gateway.tls.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

Knox IDBroker TLS/SSL Server Keystore File Password

Description

The password for the Knox IDBroker keystore file.

Related Name

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-reloadable.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-reloadable.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/gateway-reloadable.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/gateway-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Knox IDBroker AWS Credentials Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AWS Credentials Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_credentials_key

Required

true

Suppress Parameter Validation: Knox IDBroker AWS Credentials Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AWS Credentials Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_credentials_secret

Required

true

Suppress Parameter Validation: Knox IDBroker AWS Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AWS Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AWS User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AWS User Default Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_user_default_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AWS User Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AWS User Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_user_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE ADLS2 Tenant Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE ADLS2 Tenant Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_adls2_tenant_name

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE 'blob-contributor' ClientID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE 'blob-contributor' ClientID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_contributor_clientid

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE 'blob-contributor' Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE 'blob-contributor' Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_contributor_secret

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE 'blob-reader' ClientID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE 'blob-reader' ClientID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_reader_clientid

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE 'blob-reader' Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE 'blob-reader' Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_reader_secret

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE User Default Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_user_default_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE User Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE User Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_user_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker AZURE VM Assumer Identity

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker AZURE VM Assumer Identity parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_vm_assumer_identity

Required

true

Suppress Parameter Validation: Knox IDBroker Configuration Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Configuration Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_conf_dir

Required

true

Suppress Parameter Validation: Knox IDBroker Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_data_dir

Required

true

Suppress Parameter Validation: Gateway - Default App Topology Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway - Default App Topology Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_default_topology_name

Required

true

Suppress Parameter Validation: Gateway Config Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Config Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_gateway_conf_dir

Required

true

Suppress Parameter Validation: Admin Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_knox_admin_groups

Required

true

Suppress Parameter Validation: Gateway Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_path

Required

true

Suppress Parameter Validation: Gateway HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_port

Required

true

Suppress Parameter Validation: Security - Signing Key Alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Key Alias parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_key_alias

Required

true

Suppress Parameter Validation: Security - Signing Keystore Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Keystore Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_keystore_name

Required

true

Suppress Parameter Validation: Security - Signing Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Security - Signing Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_keystore_type

Required

true

Suppress Parameter Validation: Knox IDBroker GCP Credential Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker GCP Credential Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_credential_key

Required

true

Suppress Parameter Validation: Knox IDBroker GCP Credential Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker GCP Credential Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_credential_secret

Required

true

Suppress Parameter Validation: Knox IDBroker GCP Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker GCP Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker GCP User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker GCP User Default Group Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_user_default_group_mapping

Required

true

Suppress Parameter Validation: Knox IDBroker GCP User Mapping

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker GCP User Mapping parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_user_mapping

Required

true

Suppress Parameter Validation: Admin Group Mapping - Class Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Group Mapping - Class Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_hadoop_security_group_mapping_class

Required

true

Suppress Parameter Validation: IDBroker Initial/Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the IDBroker Initial/Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_heap_size

Required

true

Suppress Parameter Validation: Additional IDBroker Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional IDBroker Java Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_java_opts

Required

true

Suppress Parameter Validation: krb5.conf Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the krb5.conf Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_java_security_krb5_conf

Required

true

Suppress Parameter Validation: Kerberos Proxyuser Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Proxyuser Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_kerberos_dt_proxyuser_block

Required

true

Suppress Parameter Validation: IDBroker Master Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the IDBroker Master Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_master_secret

Required

true

Suppress Parameter Validation: Knox IDBroker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Knox IDBroker Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Knox IDBroker Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Knox IDBroker TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Knox IDBroker TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Knox IDBroker TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Knox IDBroker TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox IDBroker TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_knox_idbroker_unexpected_exits

Required

true

Service-Wide

Advanced

Knox Service Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

For advanced use only, a string to be inserted into conf/gateway-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

conf/gateway-site.xml_service_safety_valve

Required

false

Knox Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

KNOX_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

knox

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

knox

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Knox IDBroker Monitoring Thresholds

Description

The health test thresholds of the overall Knox IDBroker health. The check returns "Concerning" health if the percentage of "Healthy" Knox IDBrokers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Knox IDBrokers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

KNOX_IDBROKER_healthy_thresholds

Required

false

Healthy Knox Gateway Monitoring Thresholds

Description

The health test thresholds of the overall Knox Gateway health. The check returns "Concerning" health if the percentage of "Healthy" Knox Gateways falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Knox Gateways falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

KNOX_KNOX_GATEWAY_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Automatic Restart on Stop

Description

Automatically restart the service when a stop is issued.

Related Name

autorestart_on_stop

Default Value

false

API Name

autorestart_on_stop

Required

false

HDFS Service

Description

Name of the HDFS service that this Knox service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

Enable Kerberos Authentication

Description

Boolean flag indicating whether the Hadoop cluster protected by Gateway is secured with Kerberos

Related Name

gateway.hadoop.kerberos.secured

Default Value

false

API Name

kerberos.auth.enabled

Required

false

Knox Home Page - Hidden Topologies

Description

A comma-separated list of topology names that should not be listed in the Topologies section on the Knox Home page.

Related Name

knox.homepage.hidden.topologies

Default Value

admin manager knoxsso metadata homepage

API Name

knox_homepage_hidden_topologies

Required

false

Knox Home Page - Enable Logout

Description

Whether logout from the Knox Home page is enabled or not.

Related Name

knox.homepage.logout.enabled

Default Value

true

API Name

knox_homepage_logout_enabled

Required

false

Knox Home Page - Pinned Topologies

Description

A comma-separated list of topology names that should be auto-expanded on the Knox Home page.

Related Name

knox.homepage.pinned.topologies

Default Value

cdp-proxy

API Name

knox_homepage_pinned_topologies

Required

false

Knox PAM Realm - Service Name

Description

Using KnoxPamRealm requires a PAM service name. This is the name of the file under '/etc/pam.d' that is used to initialize and configure the PAM subsystem. Normally, this file reflects the application using it. For example 'login', 'sshd', 'su', etc...

Related Name

knox_pam_realm_service

Default Value

login

API Name

knox_pam_realm_service

Required

false

Ranger Knox Plugin Hdfs Audit Directory

Description

The HDFS path on which Ranger audits are written.

Related Name

ranger_knox_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/knox

API Name

ranger_knox_plugin_hdfs_audit_directory

Required

false

RANGER Service

Description

Name of the RANGER service that this Knox service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Save Alias Command Input

Description

This parameter serves as the input for the 'Save Alias'
command. The input must follow the following format:
topology_name_1[:topology_name_2:...:topology_name_N].alias_name=password

Related Name

save_alias_command_input_password

Default Value

API Name

save_alias_command_input_password

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

knox

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/auto-discovery-advanced-configuration-cdp-proxy-api.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy.properties

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/auto-discovery-advanced-configuration-cdp-proxy.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/auto-discovery-advanced-configuration-cdp-proxy.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/cdp-resources.xml

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/cdp-resources.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/cdp-resources.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-reloadable.xml

Description

Whether to suppress configuration warnings produced by the Knox IDBroker Advanced Configuration Snippet (Safety Valve) for conf/gateway-reloadable.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/gateway-reloadable.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/gateway-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-audit.xml

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-security.xml

Description

Whether to suppress configuration warnings produced by the Knox Gateway Advanced Configuration Snippet (Safety Valve) for conf/ranger-knox-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-knox-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Knox Simplified Topology Management - API Authentication Provider

Description

Whether to suppress configuration warnings produced by the Knox Simplified Topology Management - API Authentication Provider configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_api_authentication_provider

Required

true

Suppress Configuration Validator: Knox Gateway Configuration Directory

Description

Whether to suppress configuration warnings produced by the Knox Gateway Configuration Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_conf_dir

Required

true

Suppress Configuration Validator: Knox Gateway Data Directory

Description

Whether to suppress configuration warnings produced by the Knox Gateway Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_data_dir

Required

true

Suppress Configuration Validator: Gateway - Default App Topology Name

Description

Whether to suppress configuration warnings produced by the Gateway - Default App Topology Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_default_topology_name

Required

true

Suppress Configuration Validator: Knox Simplified Topology Management - cdp-proxy

Description

Whether to suppress configuration warnings produced by the Knox Simplified Topology Management - cdp-proxy configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_descriptor_cdp_proxy

Required

true

Suppress Configuration Validator: Knox Simplified Topology Management - cdp-proxy-api

Description

Whether to suppress configuration warnings produced by the Knox Simplified Topology Management - cdp-proxy-api configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_descriptor_cdp_proxy_api

Required

true

Suppress Configuration Validator: Knox Gateway Dispatch Whitelist

Description

Whether to suppress configuration warnings produced by the Knox Gateway Dispatch Whitelist configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_dispatch_whitelist

Required

true

Suppress Configuration Validator: Knox Gateway Dispatch Whitelist Services

Description

Whether to suppress configuration warnings produced by the Knox Gateway Dispatch Whitelist Services configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_dispatch_whitelist_services

Required

true

Suppress Configuration Validator: Gateway Config Directory

Description

Whether to suppress configuration warnings produced by the Gateway Config Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_gateway_conf_dir

Required

true

Suppress Configuration Validator: Knox Gateway Initial/Max Heapsize

Description

Whether to suppress configuration warnings produced by the Knox Gateway Initial/Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_heap_size

Required

true

Suppress Configuration Validator: Additional Gateway Java Options

Description

Whether to suppress configuration warnings produced by the Additional Gateway Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_java_opts

Required

true

Suppress Configuration Validator: Admin Groups

Description

Whether to suppress configuration warnings produced by the Admin Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_knox_admin_groups

Required

true

Suppress Configuration Validator: Knox Master Secret

Description

Whether to suppress configuration warnings produced by the Knox Master Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_master_secret

Required

true

Suppress Configuration Validator: Gateway Path

Description

Whether to suppress configuration warnings produced by the Gateway Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_path

Required

true

Suppress Configuration Validator: Gateway HTTP Port

Description

Whether to suppress configuration warnings produced by the Gateway HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_port

Required

true

Suppress Configuration Validator: Ranger Knox Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Knox Plugin Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_conf_path

Required

true

Suppress Configuration Validator: Ranger Knox Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Knox Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Knox Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Knox Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Knox Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Knox Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_knox_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Security - Signing Key Alias

Description

Whether to suppress configuration warnings produced by the Security - Signing Key Alias configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_key_alias

Required

true

Suppress Configuration Validator: Security - Signing Keystore Name

Description

Whether to suppress configuration warnings produced by the Security - Signing Keystore Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_keystore_name

Required

true

Suppress Configuration Validator: Security - Signing Keystore Type

Description

Whether to suppress configuration warnings produced by the Security - Signing Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_signing_keystore_type

Required

true

Suppress Configuration Validator: Knox Simplified Topology Management - SSO Authentication Provider

Description

Whether to suppress configuration warnings produced by the Knox Simplified Topology Management - SSO Authentication Provider configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_sso_authentication_provider

Required

true

Suppress Configuration Validator: Security - TLS Certificate Alias (Optional)

Description

Whether to suppress configuration warnings produced by the Security - TLS Certificate Alias (Optional) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_tls_certificate_alias

Required

true

Suppress Configuration Validator: Security - TLS Certificate Path (Optional)

Description

Whether to suppress configuration warnings produced by the Security - TLS Certificate Path (Optional) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_tls_certificate_path

Required

true

Suppress Configuration Validator: X-Forwarded Header Context Service Name

Description

Whether to suppress configuration warnings produced by the X-Forwarded Header Context Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gateway_xforwarded_header_context_append_servicename

Required

true

Suppress Configuration Validator: Admin Group Mapping - Class Name

Description

Whether to suppress configuration warnings produced by the Admin Group Mapping - Class Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_group_mapping_class

Required

true

Suppress Configuration Validator: Knox IDBroker AWS Credentials Key

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AWS Credentials Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_credentials_key

Required

true

Suppress Configuration Validator: Knox IDBroker AWS Credentials Secret

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AWS Credentials Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_credentials_secret

Required

true

Suppress Configuration Validator: Knox IDBroker AWS Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AWS Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AWS User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AWS User Default Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_user_default_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AWS User Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AWS User Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_aws_user_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE ADLS2 Tenant Name

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE ADLS2 Tenant Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_adls2_tenant_name

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE 'blob-contributor' ClientID

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE 'blob-contributor' ClientID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_contributor_clientid

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE 'blob-contributor' Secret

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE 'blob-contributor' Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_contributor_secret

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE 'blob-reader' ClientID

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE 'blob-reader' ClientID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_reader_clientid

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE 'blob-reader' Secret

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE 'blob-reader' Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_blob_reader_secret

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE User Default Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_user_default_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE User Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE User Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_user_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker AZURE VM Assumer Identity

Description

Whether to suppress configuration warnings produced by the Knox IDBroker AZURE VM Assumer Identity configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_azure_vm_assumer_identity

Required

true

Suppress Configuration Validator: Knox IDBroker Configuration Directory

Description

Whether to suppress configuration warnings produced by the Knox IDBroker Configuration Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_conf_dir

Required

true

Suppress Configuration Validator: Knox IDBroker Data Directory

Description

Whether to suppress configuration warnings produced by the Knox IDBroker Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_data_dir

Required

true

Suppress Configuration Validator: Gateway - Default App Topology Name

Description

Whether to suppress configuration warnings produced by the Gateway - Default App Topology Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_default_topology_name

Required

true

Suppress Configuration Validator: Gateway Config Directory

Description

Whether to suppress configuration warnings produced by the Gateway Config Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_gateway_conf_dir

Required

true

Suppress Configuration Validator: Admin Groups

Description

Whether to suppress configuration warnings produced by the Admin Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_knox_admin_groups

Required

true

Suppress Configuration Validator: Gateway Path

Description

Whether to suppress configuration warnings produced by the Gateway Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_path

Required

true

Suppress Configuration Validator: Gateway HTTP Port

Description

Whether to suppress configuration warnings produced by the Gateway HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_port

Required

true

Suppress Configuration Validator: Security - Signing Key Alias

Description

Whether to suppress configuration warnings produced by the Security - Signing Key Alias configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_key_alias

Required

true

Suppress Configuration Validator: Security - Signing Keystore Name

Description

Whether to suppress configuration warnings produced by the Security - Signing Keystore Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_keystore_name

Required

true

Suppress Configuration Validator: Security - Signing Keystore Type

Description

Whether to suppress configuration warnings produced by the Security - Signing Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gateway_signing_keystore_type

Required

true

Suppress Configuration Validator: Knox IDBroker GCP Credential Key

Description

Whether to suppress configuration warnings produced by the Knox IDBroker GCP Credential Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_credential_key

Required

true

Suppress Configuration Validator: Knox IDBroker GCP Credential Secret

Description

Whether to suppress configuration warnings produced by the Knox IDBroker GCP Credential Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_credential_secret

Required

true

Suppress Configuration Validator: Knox IDBroker GCP Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker GCP Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker GCP User Default Group Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker GCP User Default Group Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_user_default_group_mapping

Required

true

Suppress Configuration Validator: Knox IDBroker GCP User Mapping

Description

Whether to suppress configuration warnings produced by the Knox IDBroker GCP User Mapping configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_gcp_user_mapping

Required

true

Suppress Configuration Validator: Admin Group Mapping - Class Name

Description

Whether to suppress configuration warnings produced by the Admin Group Mapping - Class Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_hadoop_security_group_mapping_class

Required

true

Suppress Configuration Validator: IDBroker Initial/Max Heapsize

Description

Whether to suppress configuration warnings produced by the IDBroker Initial/Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_heap_size

Required

true

Suppress Configuration Validator: Additional IDBroker Java Options

Description

Whether to suppress configuration warnings produced by the Additional IDBroker Java Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_java_opts

Required

true

Suppress Configuration Validator: krb5.conf Location

Description

Whether to suppress configuration warnings produced by the krb5.conf Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_java_security_krb5_conf

Required

true

Suppress Configuration Validator: Kerberos Proxyuser Block

Description

Whether to suppress configuration warnings produced by the Kerberos Proxyuser Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_kerberos_dt_proxyuser_block

Required

true

Suppress Configuration Validator: IDBroker Master Secret

Description

Whether to suppress configuration warnings produced by the IDBroker Master Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_master_secret

Required

true

Suppress Configuration Validator: Knox IDBroker Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Knox IDBroker Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_idbroker_role_env_safety_valve

Required

true

Suppress Configuration Validator: krb5.conf Location

Description

Whether to suppress configuration warnings produced by the krb5.conf Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_java_security_krb5_conf

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Knox Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Knox Gateway Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_knox_gateway_role_env_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Knox Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Knox Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the Knox Gateway Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Knox Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Knox Gateway TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Knox Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Knox Gateway TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Knox Gateway TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Knox Gateway TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Knox Gateway TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Knox Gateway TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Knox Service Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Service Advanced Configuration Snippet (Safety Valve) for conf/gateway-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_conf/gateway-site.xml_service_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Configuration Validator: Knox IDBroker Count Validator

Description

Whether to suppress configuration warnings produced by the Knox IDBroker Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_idbroker_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: Knox Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Knox Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_knox_gateway_count_validator

Required

true

Suppress Parameter Validation: Knox Home Page - Hidden Topologies

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Home Page - Hidden Topologies parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_homepage_hidden_topologies

Required

true

Suppress Parameter Validation: Knox Home Page - Pinned Topologies

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Home Page - Pinned Topologies parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_homepage_pinned_topologies

Required

true

Suppress Parameter Validation: Knox PAM Realm - Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox PAM Realm - Service Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_pam_realm_service

Required

true

Suppress Parameter Validation: Knox Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_knox_service_env_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Knox Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Knox Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_knox_plugin_hdfs_audit_directory

Required

true

Suppress Parameter Validation: Save Alias Command Input

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Save Alias Command Input parameter.

Related Name

Default Value

false

API Name

service_config_suppression_save_alias_command_input_password

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Knox IDBroker Health

Description

Whether to suppress the results of the Knox IDBroker Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_knox_idbroker_healthy

Required

true

Suppress Health Test: Knox Gateway Health

Description

Whether to suppress the results of the Knox Gateway Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_knox_knox_gateway_healthy

Required

true

Kudu Properties in Cloudera Runtime 7.2.18

Role groups:

Master

Advanced

Master Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

For advanced use only. A string to be inserted into gflagfile for this role only.

Related Name

Default Value

API Name

gflagfile_role_safety_valve

Required

false

Master Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

For advanced use only. A string to be inserted into kudu-monitoring.properties for this role only.

Related Name

Default Value

API Name

kudu-monitoring.properties_role_safety_valve

Required

false

Master Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KUDU_MASTER_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-audit.xml

Description

For advanced use only. A string to be inserted into ranger-kudu-audit.xml for this role only.

Related Name

Default Value

API Name

ranger-kudu-audit.xml_role_safety_valve

Required

false

Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-kudu-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-kudu-policymgr-ssl.xml_role_safety_valve

Required

false

Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-security.xml

Description

For advanced use only. A string to be inserted into ranger-kudu-security.xml for this role only.

Related Name

Default Value

API Name

ranger-kudu-security.xml_role_safety_valve

Required

false

Logs

Master Maximum Log Level to Buffer

Description

Log messages logged at this level or lower are buffered in memory.

Related Name

logbuflevel

Default Value

0

API Name

glog_logbuflevel

Required

false

Master Maximum Log Size

Description

Approximate maximum log file size in megabytes before rolling to a new log file.

Related Name

max_log_size

Default Value

1800 MiB

API Name

glog_maxlogsize

Required

false

Master Minimum Log Level

Description

Messages logged via LOG() at a lower level than this are not logged anywhere.

Related Name

minloglevel

Default Value

0

API Name

glog_minloglevel

Required

false

Master Minimum Log Verbosity

Description

Messages logged via VLOG() at a lower verbosity than this are not logged anywhere.

Related Name

v

Default Value

0

API Name

glog_verbose

Required

false

Master Log Directory

Description

The log directory for log files of the role Master.

Related Name

log_dir

Default Value

/var/log/kudu

API Name

log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable Failed Data Directories

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KUDU-KUDU_MASTER-7.2.0-FAILED_DATA_DIRS_test_enable

Required

false

Enable Full Data Directories

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KUDU-KUDU_MASTER-7.2.0-FULL_DATA_DIRS_test_enable

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kudu_master_fd_thresholds

Required

false

Master Host Health Test

Description

When computing the overall Master health, consider the host's health.

Related Name

Default Value

true

API Name

kudu_master_host_health_enabled

Required

false

Master Process Health Test

Description

Enables the health test that the Master's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kudu_master_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.

- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Master Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

1 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Default Number of Replicas

Description

Default number of replicas for each tablet.

Related Name

default_num_replicas

Default Value

3

API Name

default_num_replicas

Required

true

Kudu Master Data Directories

Description

Directories where Kudu masters will store data blocks.

Related Name

fs_data_dirs

Default Value

API Name

fs_data_dirs

Required

true

Kudu Master WAL Directory

Description

Directory where Kudu masters will store write-ahead logs. It can be the same as one of the data directories, but not a sub-directory of a data directory. Master and tablet servers must use different directories when co-located on the same machine.

Related Name

fs_wal_dir

Default Value

API Name

fs_wal_dir

Required

true

Kudu Master WAL Fsyncs All Entries

Description

If true, the Master will use the fsync system call to ensure that all modifications to the catalog table are durably written to disk. WARNING: In this release, enabling this option can cause serious issues.

Related Name

log_force_fsync_all

Default Value

false

API Name

log_force_fsync_all

Required

true

Master Address

Description

Configuration that's automatically set by Cloudera Manager to propagate the Master's address to the Tablet Servers.

Related Name

server.address

Default Value

API Name

master_address

Required

false

Kudu Master Core Dump Directory

Description

If Enable Core Dump is set, Kudu masters will dump cores to this location.

Related Name

master_core_dump_directory

Default Value

/var/log/kudu

API Name

master_core_dump_directory

Required

true

Kudu Metrics URL Parameters

Description

The URL query parameters to append to the `/metrics` URL when collecting Kudu metrics.

Related Name

metrics_url_parameters

Default Value

compact=1&level=info

API Name

metrics_url_parameters

Required

true

Ranger Kudu Plugin Audit HDFS Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/kudu/audit/hdfs/spool

API Name

ranger_kudu_plugin_hdfs_audit_spool_directory

Required

true

Ranger Kudu Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.kudu.policy.cache.dir

Default Value

/var/lib/ranger/kudu/policy-cache

API Name

ranger_kudu_plugin_policy_cache_directory

Required

true

Ranger service name for this Kudu service

Description

Name of the Kudu Ranger service, that is used for authorization by this Kudu service. If this parameter is set to the placeholder value '{{GENERATED_RANGER_SERVICE_NAME}}', a generated service name will be used, and if necessary, created. The generated service name will refer to the name of the cluster and the name of this Kudu service. The name can consist of alphanumeric and '_' characters.

Related Name

ranger.plugin.kudu.service.name

Default Value

cm_kudu

API Name

ranger_kudu_plugin_service_name

Required

false

Ranger Kudu Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/kudu/audit/solr/spool

API Name

ranger_kudu_plugin_solr_audit_spool_directory

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.kudu.trusted.proxy.ipaddress

Default Value

API Name

ranger_kudu_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.kudu.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_kudu_plugin_use_x_forwarded_for_ipaddress

Required

false

Kudu Master Web UI Interface

Description

The interface of the Kudu Master Web UI. If blank, binds to 0.0.0.0.

Related Name

webserver_interface

Default Value

API Name

webserver_interface

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Kudu Master Web UI Port

Description

The port of the Kudu Master Web UI.

Related Name

webserver_port

Default Value

8051

API Name

webserver_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Master TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Master might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

kudu.ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Master TLS/SSL Trust Store Password

Description

The password for the Master TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

kudu.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Master

Description

Encrypt communication between clients and Master using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Master TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Master is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Master TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Master is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_certificate_file

Default Value

API Name

ssl_server_certificate_location

Required

false

Master TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Master is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_private_key_file

Default Value

API Name

ssl_server_privatekey_location

Required

false

Master TLS/SSL Private Key Password

Description

The password for the private key in the Master TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

webserver_private_key_password_cmd

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Default Number of Replicas

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Number of Replicas parameter.

Related Name

Default Value

false

API Name

role_config_suppression_default_num_replicas

Required

true

Suppress Parameter Validation: Kudu Master Data Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Master Data Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fs_data_dirs

Required

true

Suppress Parameter Validation: Kudu Master WAL Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Master WAL Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fs_wal_dir

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for gflagfile parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gflagfile_role_safety_valve

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kudu-monitoring.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Master Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kudu_master_role_env_safety_valve

Required

true

Suppress Parameter Validation: Master Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Master Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_master_address

Required

true

Suppress Parameter Validation: Kudu Master Core Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Master Core Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_master_core_dump_directory

Required

true

Suppress Parameter Validation: Kudu Metrics URL Parameters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Metrics URL Parameters parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics_url_parameters

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Kudu Plugin Audit HDFS Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kudu Plugin Audit HDFS Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Kudu Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kudu Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger service name for this Kudu service

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger service name for this Kudu service parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_service_name

Required

true

Suppress Parameter Validation: Ranger Kudu Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kudu Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Master TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Master TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Master TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Master TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Master TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Master TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Master TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Parameter Validation: Kudu Master Web UI Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Master Web UI Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_interface

Required

true

Suppress Parameter Validation: Kudu Master Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Master Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_port

Required

true

Suppress Health Test: Failed Data Directories

Description

Whether to suppress the results of the Failed Data Directories heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu-kudu_master-7.2.0-failed_data_dirs

Required

true

Suppress Health Test: Full Data Directories

Description

Whether to suppress the results of the Full Data Directories heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu-kudu_master-7.2.0-full_data_dirs

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_master_unexpected_exits

Required

true

Service-Wide

Advanced

Kudu Service Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

For advanced use only, a string to be inserted into gflagfile. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

gflagfile_service_safety_valve

Required

false

Kudu Service Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

For advanced use only, a string to be inserted into kudu-monitoring.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

kudu-monitoring.properties_service_safety_valve

Required

false

Kudu Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

KUDU_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

kudu

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

kudu

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Master Monitoring Thresholds

Description

The health test thresholds of the overall Master health. The check returns "Concerning" health if the percentage of "Healthy" Masters falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Masters falls below the critical threshold.

Related Name

Default Value

Warning: 80.1 %, Critical: 60.0 %

API Name

KUDU_KUDU_MASTER_healthy_thresholds

Required

false

Healthy Tablet Server Monitoring Thresholds

Description

The health test thresholds of the overall Tablet Server health. The check returns "Concerning" health if the percentage of "Healthy" Tablet Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Tablet Servers falls below the critical threshold.

Related Name

Default Value

Warning: 75.0 %, Critical: 50.0 %

API Name

KUDU_KUDU_TSERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Time Servers for Built-In NTP Client

Description

Comma-separated list of NTP servers to use for the built-in NTP client, in format [FQDN|IPv4] [:PORT]. These are only used if the 'builtin' Time Source is selected.

Related Name

builtin_ntp_servers

Default Value

0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org

API Name

builtin_ntp_servers

Required

false

Enable Core Dump

Description

Used to generate a core dump to get more information about a Kudu crash. Unless otherwise configured systemwide using /proc/sys/kernel/core_pattern, the dump is generated in the configured core dump directory. The core file can be very large.

Related Name

enable_core_dump

Default Value

false

API Name

enable_core_dump

Required

true

Enable Secure Authentication, Encryption, And Web UI

Description

Enable secure authentication and encryption between all Kudu clients and servers as well as between individual servers. Also enables secure authentication in every Kudu server's web UI. Kerberos must be configured.

Related Name

enable_security

Default Value

false

API Name

enable_security

Required

true

HDFS Service

Description

Name of the HDFS service that this Kudu service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

HMS Service

Description

Name of the HMS service that this Kudu service instance depends on

Related Name

Default Value

API Name

hms_service

Required

false

Ranger Kudu Plugin Hdfs Audit Directory

Description

The HDFS path on which Ranger audits are written.

Related Name

ranger_kudu_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/kudu

API Name

ranger_kudu_plugin_hdfs_audit_directory

Required

false

RANGER Service

Description

Name of the RANGER service that this Kudu service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Maximum Number of Per-tablet-server Replica Moves

Description

Maximum number of replica moves to perform concurrently on one tablet server: moves of replicas to the server and moves of replicas off of the server count against this limit.

Related Name

rb_max_moves_per_server

Default Value

5

API Name

rb_max_moves_per_server

Required

false

Maximum Allowed Runtime of the Rebalancing Tool

Description

Maximum time to run the rebalancing, in seconds. Specifying 0 means not imposing any limit on the rebalancing run time.

Related Name

rb_max_run_time_sec

Default Value

0

API Name

rb_max_run_time_sec

Required

false

Maximum Allowed Duration Without Rebalancer Progress

Description

Maximum duration of the 'staleness' interval where the rebalance can not make progress. If this period elapses without the rebalancer making progress, it will exit indicating failure. This may happen in case of a persistent problem with the cluster or when some unexpected concurrent activity is present (such as automatic recovery of failed replicas, etc.)

Related Name

rb_max_staleness_interval_sec

Default Value

300

API Name

rb_max_staleness_interval_sec

Required

false

Maximum Allowed Runtime to Rolling Restart a Batch of Servers

Description

Maximum time to allow for the restart of a batch of servers during a rolling restart. If this period elapses without the cluster becoming healthy, the rolling restart will exit indicating failure. This may happen if there is a persistent problem with the cluster.

Related Name

rr_batch_time_limit_sec

Default Value

1800

API Name

rr_batch_time_limit_sec

Required

false

Rolling Restart Health Check Interval

Description

Interval in seconds with which to check the health of a cluster in waiting for a server or batch of servers to come back online, before moving onto the next server or batch of servers during a rolling restart.

Related Name

rr_health_check_interval_sec

Default Value

60

API Name

rr_health_check_interval_sec

Required

false

Sentry Service

Description

Name of the Sentry service that this Kudu service instance depends on

Related Name

Default Value

API Name

sentry_service

Required

false

Superuser Access Control List

Description

The list of usernames to allow as super users, comma-separated. A '*' entry indicates that all authenticated users are allowed. If this is left unset or blank, the default behavior is that the identity of the daemon itself determines the superuser. If the daemon is logged in from a Keytab, then the local username from the Kerberos principal is used; otherwise, the local Unix username is used.

Related Name

superuser_acl

Default Value

API Name

superuser_acl

Required

false

Time Source

Description

Time source for HybridClock timestamps. If set to 'auto', Kudu selects the best available time source for the environment: for particular public cloud types, Kudu uses the dedicated NTP server available from within a public cloud instance, otherwise, Kudu relies on the local system clock to be synchronized by NTP. If set to 'builtin', Kudu masters and tablet servers use the built-in NTP client, where the set of servers is configured as specified by the 'Servers for Built-in NTP Client' configuration property (--builtin_ntp_servers flag). If set to 'system', Kudu relies on the local system clock to be synchronized by NTP, where the synchronization by NTP is a requirement.

Related Name

time_source

Default Value

system

API Name

time_source

Required

true

User Access Control List

Description

The list of usernames who may access the cluster, comma-separated. A '*' entry indicates that all authenticated users are allowed.

Related Name

user_acl

Default Value

*

API Name

user_acl

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

kudu

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: Kudu Tablet Server Block Cache Capacity

Description

Whether to suppress configuration warnings produced by the Kudu Tablet Server Block Cache Capacity configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_block_cache_capacity_mb

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Default Number of Replicas

Description

Whether to suppress configuration warnings produced by the Default Number of Replicas configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_default_num_replicas

Required

true

Suppress Configuration Validator: Kudu Master Data Directories

Description

Whether to suppress configuration warnings produced by the Kudu Master Data Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fs_data_dirs

Required

true

Suppress Configuration Validator: Kudu Master WAL Directory

Description

Whether to suppress configuration warnings produced by the Kudu Master WAL Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_fs_wal_dir

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for gflagfile configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gflagfile_role_safety_valve

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kudu-monitoring.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Master Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Master Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kudu_master_role_env_safety_valve

Required

true

Suppress Configuration Validator: Tablet Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Tablet Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kudu_tserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: Master Log Directory

Description

Whether to suppress configuration warnings produced by the Master Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Kudu Tablet Server Maintenance Threads

Description

Whether to suppress configuration warnings produced by the Kudu Tablet Server Maintenance Threads configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_maintenance_manager_num_threads

Required

true

Suppress Configuration Validator: Master Address

Description

Whether to suppress configuration warnings produced by the Master Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_master_address

Required

true

Suppress Configuration Validator: Kudu Master Core Dump Directory

Description

Whether to suppress configuration warnings produced by the Kudu Master Core Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_master_core_dump_directory

Required

true

Suppress Configuration Validator: Kudu Tablet Server Hard Memory Limit

Description

Whether to suppress configuration warnings produced by the Kudu Tablet Server Hard Memory Limit configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_memory_limit_hard_bytes

Required

true

Suppress Configuration Validator: Kudu Metrics URL Parameters

Description

Whether to suppress configuration warnings produced by the Kudu Metrics URL Parameters configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metrics_url_parameters

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-audit.xml

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-security.xml

Description

Whether to suppress configuration warnings produced by the Master Advanced Configuration Snippet (Safety Valve) for ranger-kudu-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kudu-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Kudu Plugin Audit HDFS Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kudu Plugin Audit HDFS Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Kudu Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kudu Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger service name for this Kudu service

Description

Whether to suppress configuration warnings produced by the Ranger service name for this Kudu service configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_service_name

Required

true

Suppress Configuration Validator: Ranger Kudu Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Kudu Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kudu_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Master TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Master TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Master TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Server CA Certificate (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Configuration Validator: Master TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Configuration Validator: Master TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Configuration Validator: Master TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Master TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Configuration Validator: Kudu Tablet Server Core Dump Directory

Description

Whether to suppress configuration warnings produced by the Kudu Tablet Server Core Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_tserver_core_dump_directory

Required

true

Suppress Configuration Validator: Kudu Master Web UI Interface

Description

Whether to suppress configuration warnings produced by the Kudu Master Web UI Interface configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_interface

Required

true

Suppress Configuration Validator: Kudu Master Web UI Port

Description

Whether to suppress configuration warnings produced by the Kudu Master Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_port

Required

true

Suppress Parameter Validation: Time Servers for Built-In NTP Client

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Time Servers for Built-In NTP Client parameter.

Related Name

Default Value

false

API Name

service_config_suppression_builtin_ntp_servers

Required

true

Suppress Parameter Validation: Kudu Service Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Service Advanced Configuration Snippet (Safety Valve) for gflagfile parameter.

Related Name

Default Value

false

API Name

service_config_suppression_gflagfile_service_safety_valve

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Kudu Service Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Service Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kudu-monitoring.properties_service_safety_valve

Required

true

Suppress Configuration Validator: Master Count Validator

Description

Whether to suppress configuration warnings produced by the Master Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kudu_master_count_validator

Required

true

Suppress Parameter Validation: Kudu Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kudu_service_env_safety_valve

Required

true

Suppress Configuration Validator: Tablet Server Count Validator

Description

Whether to suppress configuration warnings produced by the Tablet Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_kudu_tserver_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Kudu Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Kudu Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kudu_plugin_hdfs_audit_directory

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Superuser Access Control List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Superuser Access Control List parameter.

Related Name

Default Value

false

API Name

service_config_suppression_superuser_acl

Required

true

Suppress Parameter Validation: User Access Control List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the User Access Control List parameter.

Related Name

Default Value

false

API Name

service_config_suppression_user_acl

Required

true

Suppress Health Test: Master Health

Description

Whether to suppress the results of the Master Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_kudu_kudu_master_healthy

Required

true

Suppress Health Test: Tablet Server Health

Description

Whether to suppress the results of the Tablet Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_kudu_kudu_tserver_healthy

Required

true

Tablet Server

Advanced

Tablet Server Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

For advanced use only. A string to be inserted into gflagfile for this role only.

Related Name

Default Value

API Name

gflagfile_role_safety_valve

Required

false

Tablet Server Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

For advanced use only. A string to be inserted into kudu-monitoring.properties for this role only.

Related Name

Default Value

API Name

kudu-monitoring.properties_role_safety_valve

Required

false

Tablet Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

KUDU_TSERVER_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Tablet Server Maximum Log Level to Buffer

Description

Log messages logged at this level or lower are buffered in memory.

Related Name

logbuflevel

Default Value

0

API Name

glog_logbuflevel

Required

false

Tablet Server Maximum Log Size

Description

Approximate maximum log file size in megabytes before rolling to a new log file.

Related Name

max_log_size

Default Value

1800 MiB

API Name

glog_maxlogsize

Required

false

Tablet Server Minimum Log Level

Description

Messages logged via LOG() at a lower level than this are not logged anywhere.

Related Name

minloglevel

Default Value

0

API Name

glog_minloglevel

Required

false

Tablet Server Minimum Log Verbosity

Description

Messages logged via VLOG() at a lower verbosity than this are not logged anywhere.

Related Name

v

Default Value

0

API Name

glog_verbose

Required

false

Tablet Server Log Directory

Description

The log directory for log files of the role Tablet Server.

Related Name

log_dir

Default Value

/var/log/kudu

API Name

log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable Failed Data Directories

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KUDU-KUDU_TSERVER-7.2.0-FAILED_DATA_DIRS_test_enable

Required

false

Enable Full Data Directories

Description

Enables or disables the health test. When disabled, the test does not run at all, nor generate health history.

Related Name

Default Value

true

API Name

KUDU-KUDU_TSERVER-7.2.0-FULL_DATA_DIRS_test_enable

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

kudu_tserver_fd_thresholds

Required

false

Tablet Server Host Health Test

Description

When computing the overall Tablet Server health, consider the host's health.

Related Name

Default Value

true

API Name

kudu_tserver_host_health_enabled

Required

false

Tablet Server Process Health Test

Description

Enables the health test that the Tablet Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

kudu_tserver_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Kudu Tablet Server Block Cache Capacity

Description

Maximum amount of memory allocated to the Kudu Tablet Server's block cache.

Related Name

block_cache_capacity_mb

Default Value

512 MiB

API Name

block_cache_capacity_mb

Required

true

Tablet Server Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

1 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Kudu Tablet Server Data Directories

Description

Directories where Kudu tablet servers will store data blocks.

Related Name

fs_data_dirs

Default Value

API Name

fs_data_dirs

Required

true

Kudu Tablet Server WAL Directory

Description

Directory where Kudu tablet servers will store write-ahead logs. It can be the same as one of the data directories, but not a sub-directory of a data directory. Master and tablet servers must use different directories when co-located on the same machine.

Related Name

fs_wal_dir

Default Value

API Name

fs_wal_dir

Required

true

Kudu Tablet Server WAL Fsyncs All Entries

Description

If true, the Tablet Server will use the fsync system call to ensure that all writes are durably written to to the write-ahead log (WAL) before responding. If false, edits will be written to the Linux buffer cache on a majority of replicas before responding.

Related Name

log_force_fsync_all

Default Value

false

API Name

log_force_fsync_all

Required

true

Kudu Tablet Server Maintenance Threads

Description

The number of threads devoted to background maintenance operations such as flushes and compactions. If the tablet server appears to be falling behind on write operations (inserts, updates, and deletes) but CPU and disk resources are not saturated, increasing this thread count will devote more resources to these background operations.

Related Name

maintenance_manager_num_threads

Default Value

1

API Name

maintenance_manager_num_threads

Required

true

Kudu Tablet Server Hard Memory Limit

Description

Maximum amount of memory that the Kudu Tablet Server will use before it starts rejecting all incoming writes.

Related Name

memory_limit_hard_bytes

Default Value

4 GiB

API Name

memory_limit_hard_bytes

Required

true

Kudu Metrics URL Parameters

Description

The URL query parameters to append to the `/metrics` URL when collecting Kudu metrics.

Related Name

metrics_url_parameters

Default Value

compact=1&level=info

API Name

metrics_url_parameters

Required

true

Tablet History Max Age

Description

The maximum amount of time, in seconds, to preserve tablet data history, including history required to perform diff scans and incremental backups. The duration defined by this parameter is also the maximum amount of time it is possible to wait after a full or incremental backup before performing the next incremental backup. Setting the value to -1 disables history removal.

Related Name

tablet_history_max_age_sec

Default Value

7 day(s)

API Name

tablet_history_max_age_sec

Required

true

Tablet Server Quiescing Interval

Description

Interval in seconds with which to check whether a Tablet Server has fully quiesced

Related Name

ts_quiescing_retry_interval_sec

Default Value

30

API Name

ts_quiescing_retry_interval_sec

Required

false

Maximum Allowed Runtime to Quiesce a Tablet Server

Description

Maximum time to wait for a Tablet Server to fully quiesce, relinquishing leadership of all Tablets and completion of all active scans.

Related Name

ts_quiescing_time_limit_sec

Default Value

1800

API Name

ts_quiescing_time_limit_sec

Required

false

Kudu Tablet Server Core Dump Directory

Description

If Enable Core Dump is set, Kudu Tablet Servers will dump cores to this location.

Related Name

tserver_core_dump_directory

Default Value

/var/log/kudu

API Name

tserver_core_dump_directory

Required

true

Kudu Tablet Server Web UI Interface

Description

The interface of the Kudu Tablet Server Web UI. If blank, binds to 0.0.0.0.

Related Name

webserver_interface

Default Value

API Name

webserver_interface

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Kudu Tablet Server Web UI Port

Description

The port of the Kudu Tablet Server Web UI.

Related Name

webserver_port

Default Value

8050

API Name

webserver_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable TLS/SSL for Tablet Server

Description

Encrypt communication between clients and Tablet Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Tablet Server TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Tablet Server is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Tablet Server TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Tablet Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_certificate_file

Default Value

API Name

ssl_server_certificate_location

Required

false

Tablet Server TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Tablet Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

webserver_private_key_file

Default Value

API Name

ssl_server_privatekey_location

Required

false

Tablet Server TLS/SSL Private Key Password

Description

The password for the private key in the Tablet Server TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

webserver_private_key_password_cmd

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Parameter Validation: Kudu Tablet Server Block Cache Capacity

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Block Cache Capacity parameter.

Related Name

Default Value

false

API Name

role_config_suppression_block_cache_capacity_mb

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Kudu Tablet Server Data Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Data Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fs_data_dirs

Required

true

Suppress Parameter Validation: Kudu Tablet Server WAL Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server WAL Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_fs_wal_dir

Required

true

Suppress Parameter Validation: Tablet Server Advanced Configuration Snippet (Safety Valve) for gflagfile

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server Advanced Configuration Snippet (Safety Valve) for gflagfile parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gflagfile_role_safety_valve

Required

true

Suppress Parameter Validation: Tablet Server Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server Advanced Configuration Snippet (Safety Valve) for kudu-monitoring.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kudu-monitoring.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Tablet Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kudu_tserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: Tablet Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Kudu Tablet Server Maintenance Threads

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Maintenance Threads parameter.

Related Name

Default Value

false

API Name

role_config_suppression_maintenance_manager_num_threads

Required

true

Suppress Parameter Validation: Kudu Tablet Server Hard Memory Limit

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Hard Memory Limit parameter.

Related Name

Default Value

false

API Name

role_config_suppression_memory_limit_hard_bytes

Required

true

Suppress Parameter Validation: Kudu Metrics URL Parameters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Metrics URL Parameters parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics_url_parameters

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Tablet Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Tablet Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Tablet Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Tablet Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tablet Server TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Parameter Validation: Kudu Tablet Server Core Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Core Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_tserver_core_dump_directory

Required

true

Suppress Parameter Validation: Kudu Tablet Server Web UI Interface

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Web UI Interface parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_interface

Required

true

Suppress Parameter Validation: Kudu Tablet Server Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kudu Tablet Server Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_webserver_port

Required

true

Suppress Health Test: Failed Data Directories

Description

Whether to suppress the results of the Failed Data Directories heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu-kudu_tserver-7.2.0-failed_data_dirs

Required

true

Suppress Health Test: Full Data Directories

Description

Whether to suppress the results of the Full Data Directories heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu-kudu_tserver-7.2.0-full_data_dirs

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_kudu_kudu_tserver_unexpected_exits

Required

true

Livy Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/livy

API Name

client_config_root_dir

Required

true

Livy Client Advanced Configuration Snippet (Safety Valve) for livy-conf/livy-client.conf

Description

For advanced use only, a string to be inserted into the client configuration for livy-conf/livy-client.conf.

Related Name

Default Value

API Name

livy-conf/livy-client.conf_client_config_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Security

Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

livy.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Gateway TLS/SSL Trust Store Password

Description

The password for the Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

livy.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Livy Client Advanced Configuration Snippet (Safety Valve) for livy-conf/livy-client.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Client Advanced Configuration Snippet (Safety Valve) for livy-conf/livy-client.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy-conf/livy-client.conf_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Livy Server

Advanced

Livy Server Advanced Configuration Snippet (Safety Valve) for livy-conf/livy.conf

Description

For advanced use only. A string to be inserted into livy-conf/livy.conf for this role only.

Related Name

Default Value

API Name

livy-conf/livy.conf_role_safety_valve

Required

false

Livy Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

LIVY_SERVER_role_env_safety_valve

Required

false

Livy Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Livy Server Log Directory

Description

The log directory for log files of the role Livy Server.

Related Name

log_dir

Default Value

/var/log/livy

API Name

log_dir

Required

false

Livy Server Logging Threshold

Description

The minimum log level for Livy Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Livy Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Livy Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Livy Server Max Log Size

Description

The maximum size, in megabytes, per log file for Livy Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

livy_server_fd_thresholds

Required

false

Livy Server Host Health Test

Description

When computing the overall Livy Server health, consider the host's health.

Related Name

Default Value

true

API Name

livy_server_host_health_enabled

Required

false

Livy Server Process Health Test

Description

Enables the health test that the Livy Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

livy_server_scm_health_enabled

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Access Control

Description

Perform access control when processing user requests.

Related Name

livy.server.access-control.enabled

Default Value

true

API Name

livy_access_control_enabled

Required

false

Admin Users

Description

List of users with admin permissions (can view and modify any session).

Related Name

livy.superusers

Default Value

knox zeppelin

API Name

livy_admin_users

Required

false

Extra JVM Options

Description

Command line options to add to the Livy Server JVM. May be used also to override options automatically added by CM.

Related Name

livy_extra_java_opts

Default Value

API Name

livy_extra_java_opts

Required

false

Enable User Impersonation

Description

Start applications as the requesting user, instead of using the Livy account.

Related Name

livy.impersonation.enabled

Default Value

true

API Name

livy_impersonation_enabled

Required

false

Max Header Size

Description

Maximum size of a header field accepted by the Livy server. May need to be increased in certain environments where SPNEGO is enabled.

Related Name

livy.server.request-header.size

Default Value

128 KiB

API Name

livy_max_header_size

Required

false

Java Heap Size of Livy Server

Description

Maximum size for the Java process heap memory.

Related Name

livy_max_heapsize

Default Value

512 MiB

API Name

livy_max_heapsize

Required

false

Enable RPC Encryption

Description

Enable encryption of communication between the Livy session and managed Spark sessions.

Related Name

livy_rpc_encryption_enabled

Default Value

true

API Name

livy_rpc_encryption_enabled

Required

false

Enable Livy Thrift Server

Description

Enables the Livy Thrift server

Related Name

livy.server.thrift.enabled

Default Value

false

API Name

livy_server_thrift_enabled

Required

false

Livy Thrift Server Transport Mode

Description

Transport mode used by the Livy Thrift server

Related Name

livy.server.thrift.transport.mode

Default Value

binary

API Name

livy_server_thrift_transport_mode

Required

false

Enable Session Recovery

Description

Enable recovery of live sessions when the Livy server restarts. Uses HDFS to store recovery information.

Related Name

livy_session_recovery_enabled

Default Value

true

API Name

livy_session_recovery_enabled

Required

false

Enable User Authentication

Description

Enables user authentication using SPNEGO when Kerberos is enabled.

Related Name

livy_spnego_enabled

Default Value

true

API Name

livy_spnego_enabled

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Livy Server Port

Description

The port of the Livy server

Related Name

livy.server.port

Default Value

8998

API Name

livy_server_port

Required

false

Livy Thrift Server Port

Description

The port of the Livy Thrift server

Related Name

livy.server.thrift.port

Default Value

10090

API Name

livy_server_thrift_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable TLS/SSL for Livy Server

Description

Encrypt communication between clients and Livy Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

livy.tls.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Livy Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Livy Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

livy.keystore

Default Value

API Name

ssl_server_keystore_location

Required

false

Livy Server TLS/SSL Server Keystore File Password

Description

The password for the Livy Server keystore file.

Related Name

livy.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Livy Server Advanced Configuration Snippet (Safety Valve) for livy-conf/livy.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server Advanced Configuration Snippet (Safety Valve) for livy-conf/livy.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy-conf/livy.conf_role_safety_valve

Required

true

Suppress Parameter Validation: Admin Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy_admin_users

Required

true

Suppress Parameter Validation: Extra JVM Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Extra JVM Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy_extra_java_opts

Required

true

Suppress Parameter Validation: Livy Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_port

Required

true

Suppress Parameter Validation: Livy Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Livy Thrift Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Thrift Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_thrift_port

Required

true

Suppress Parameter Validation: Livy Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Livy Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Livy Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Livy Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_livy_livy_server_unexpected_exits

Required

true

Service-Wide

Advanced

Livy Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

LIVY_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

livy

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

livy

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Livy Server Role Health Test

Description

When computing the overall LIVY health, consider Livy Server's health

Related Name

Default Value

true

API Name

LIVY_LIVY_SERVER_health_enabled

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "I F (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "

streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HMS Service

Description

Name of the HMS service that this Livy service instance depends on

Related Name

Default Value

API Name

hms_service

Required

false

Recovery Directory (HDFS)

Description

Location where to store recovery metadata.

Related Name

livy.server.recovery.state-store.url

Default Value

/user/livy/recovery

API Name

livy_recovery_dir

Required

false

SPARK_ON_YARN Service

Description

Name of the SPARK_ON_YARN service that this Livy service instance depends on

Related Name

Default Value

API Name

spark_on_yarn_service

Required

true

YARN Service

Description

Name of the YARN service that this Livy service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

livy

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Livy Client Advanced Configuration Snippet (Safety Valve) for livy-conf/livy-client.conf

Description

Whether to suppress configuration warnings produced by the Livy Client Advanced Configuration Snippet (Safety Valve) for livy-conf/livy-client.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy-conf/livy-client.conf_client_config_safety_valve

Required

true

Suppress Configuration Validator: Livy Server Advanced Configuration Snippet (Safety Valve) for livy-conf/livy.conf

Description

Whether to suppress configuration warnings produced by the Livy Server Advanced Configuration Snippet (Safety Valve) for livy-conf/livy.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy-conf/livy.conf_role_safety_valve

Required

true

Suppress Configuration Validator: Admin Users

Description

Whether to suppress configuration warnings produced by the Admin Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy_admin_users

Required

true

Suppress Configuration Validator: Extra JVM Options

Description

Whether to suppress configuration warnings produced by the Extra JVM Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy_extra_java_opts

Required

true

Suppress Configuration Validator: Livy Server Port

Description

Whether to suppress configuration warnings produced by the Livy Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_port

Required

true

Suppress Configuration Validator: Livy Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Livy Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Livy Thrift Server Port

Description

Whether to suppress configuration warnings produced by the Livy Thrift Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_livy_server_thrift_port

Required

true

Suppress Configuration Validator: Livy Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Livy Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Livy Server Log Directory

Description

Whether to suppress configuration warnings produced by the Livy Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Gateway TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Gateway TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Livy Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Livy Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Livy Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Livy Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Recovery Directory (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recovery Directory (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_livy_recovery_dir

Required

true

Suppress Configuration Validator: Livy Server Count Validator

Description

Whether to suppress configuration warnings produced by the Livy Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_livy_server_count_validator

Required

true

Suppress Parameter Validation: Livy Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_livy_service_env_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Livy Server Health

Description

Whether to suppress the results of the Livy Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_livy_livy_livy_server_health

Required

true

Oozie Properties in Cloudera Runtime 7.2.18

Role groups:

Oozie Server

Advanced

Oozie Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Oozie Server Advanced Configuration Snippet (Safety Valve) for action-conf/default.xml

Description

For advanced use only. A string to be inserted into action-conf/default.xml for this role only.

Related Name

Default Value

API Name

oozie_action_config_default_safety_valve

Required

false

Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml

Description

For advanced use only. A string to be inserted into oozie-site.xml for this role only.

Related Name

Default Value

API Name

oozie_config_safety_valve

Required

false

Oozie ActionService Executor Extension Classes

Description

Comma-separated list of ActionService executor extension classes. Only action types with associated executors can be used in workflows. For CDH 5.4 and higher, this parameter is used only to specify additional classes for workflows. All executor extension classes included in that release will be added automatically and do not need to be specified.

Related Name

oozie.service.ActionService.executor.ext.classes

Default Value

API Name

oozie_executor_extension_classes

Required

false

Java Configuration Options for Oozie Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

-XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -XX:G1HeapRegionSize=16M -XX:MinMetaspaceFreeRatio=50 -XX:MaxMetaspaceFreeRatio=80 -XX:+DisableExplicitGC

API Name

oozie_java_opts

Required

false

Directory For JSP Temp Files

Description

Directory to use to for temporary JSP file storage.

Related Name

oozie.jsp.tmp.dir

Default Value

/tmp

API Name

oozie_jsp_tmp_dir

Required

false

Default Launcher Max Attempts

Description

The default YARN maximal attempt count of the Launcher ApplicationMaster.

Related Name

oozie.launcher.default.max.attempts

Default Value

2

API Name

oozie_launcher_default_max_attempts

Required

false

Default Launcher Memory

Description

The default amount of memory in MiB that is allocated for the Launcher ApplicationMasters.

Related Name

oozie.launcher.default.memory.mb

Default Value

2 GiB

API Name

oozie_launcher_default_memory

Required

false

Default Launcher Queue

Description

The default YARN pool where the Launcher ApplicationMaster is placed.

Related Name

oozie.launcher.default.queue

Default Value

default

API Name

oozie_launcher_default_queue

Required

false

Oozie Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

OOZIE_SERVER_role_env_safety_valve

Required

false

Oozie HTTP Request Header Size

Description

Controls the size of the HTTP request header.

Related Name

oozie.http.request.header.size

Default Value

64 KiB

API Name

oozie_service_http_request_header_size

Required

false

Oozie HTTP Response Header Size

Description

Controls the size of the HTTP response header.

Related Name

oozie.http.response.header.size

Default Value

64 KiB

API Name

oozie_service_http_response_header_size

Required

false

Oozie SchemaService Workflow Extension Schemas

Description

Comma-separated list of SchemaService workflow extension schemas for additional action types. From CDH 5.4 and higher, this parameter is used only to specify additional schemas for workflows. All schemas included in that release will be added automatically and do not need to be specified.

Related Name

oozie.service.SchemaService.wf.ext.schemas

Default Value

API Name

oozie_workflow_extension_schemas

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Database

Oozie Server Data Directory

Description

Directory where the Oozie Server places its data. Only applicable when using Derby as the database type.

Related Name

Default Value

/var/lib/oozie/data

API Name

oozie_data_dir

Required

false

Oozie Database Connection Properties

Description

Properties to set on the database connection directly. See oozie_datasource_properties for setting properties on the Datasouorce object.

Related Name

Default Value

API Name

oozie_database_connection_properties

Required

false

Oozie Server Database Host

Description

Hostname of the database used by Oozie Server. If the port is non-default for your database type, use host:port notation. Does not apply if you are using Derby as the database type.

Related Name

Default Value

localhost

API Name

oozie_database_host

Required

false

Oozie Server Database Is Secure

Description

Whether Oozie should connect to its database through a secure connection or not

Related Name

Default Value

false

API Name

oozie_database_is_secure

Required

false

Oozie Server Database Name

Description

Name of the database used by Oozie Server.

Related Name

Default Value

oozie

API Name

oozie_database_name

Required

false

Oozie Server Database Password

Description

Password for connecting to the database used by Oozie Server. Does not apply if you are using Derby as the database type.

Related Name

oozie.service.JPAService.jdbc.password

Default Value

API Name

oozie_database_password

Required

false

Oozie Server Database Type

Description

Type of the database used by Oozie Server.

Related Name

Default Value

derby

API Name

oozie_database_type

Required

false

Oozie Server Database User

Description

Username for connecting to the database used by Oozie Server. Does not apply if you are using Derby as the database type.

Related Name

oozie.service.JPAService.jdbc.username

Default Value

sa

API Name

oozie_database_user

Required

false

Oozie Datasource Properties

Description

Properties to set on the Datasource object (e.g.: lock timeout). NOTE: This will not be set on the database connection, but on the Datasource object wrapping the connection. See also: oozie_database_connection_properties.

Related Name

Default Value

API Name

oozie_datasource_properties

Required

false

Logs

Oozie Server Logging Threshold

Description

The minimum log level for Oozie Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Oozie Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Oozie Server logs. Typically used by log4j or logback.

Related Name

Default Value

720

API Name

max_log_backup_index

Required

false

Oozie Server Log Directory

Description

Directory where Oozie Server will place its log files.

Related Name

Default Value

/var/log/oozie

API Name

oozie_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Workflow Status Metrics Collection Interval

Description

Workflow Status metrics collection interval.

Related Name

oozie.service.DBLiteWorkflowStoreService.status.metrics.collection.interval

Default Value

1 minute(s)

API Name

oozie_job_metric_collection_interval

Required

false

Oozie Server Callable Queue Monitoring Threshold

Description

The health test thresholds of the weighted average size of the Oozie Server callable queue over a recent period. See also Oozie Server Callable Queue Monitoring Period.

Related Name

Default Value

Warning: 80.0 %, Critical: 95.0 %

API Name

oozie_server_callable_queue_threshold

Required

false

Oozie Server Callable Queue Monitoring Period

Description

The period over which to compute the moving average of the callable queue size.

Related Name

Default Value

5 minute(s)

API Name

oozie_server_callable_queue_window

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

oozie_server_fd_thresholds

Required

false

Oozie Server Host Health Test

Description

When computing the overall Oozie Server health, consider the host's health.

Related Name

Default Value

true

API Name

oozie_server_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

oozie_server_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

oozie_server_pause_duration_window

Required

false

Oozie Server Process Health Test

Description

Enables the health test that the Oozie Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

oozie_server_scm_health_enabled

Required

false

Enable Oozie Server Shared Libraries Version Check

Description

If true, enables version check for Oozie Server and installed shared libraries.

Related Name

Default Value

true

API Name

oozie_server_shared_lib_version_check_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

oozie_server_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

oozie_server_web_metric_collection_thresholds

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Oozie Email Action From Address

Description

The from address to be used for mailing all emails for Oozie email action

Related Name

oozie.email.from.address

Default Value

oozie@localhost

API Name

oozie_email_from_address

Required

false

Oozie Email Action SMTP Authentication Enabled

Description

Enable SMTP authentication for Oozie email action

Related Name

oozie.email.smtp.auth

Default Value

false

API Name

oozie_email_smtp_auth

Required

false

Oozie Email Action SMTP Host

Description

The SMTP server host to use for Oozie email action

Related Name

oozie.email.smtp.host

Default Value

localhost

API Name

oozie_email_smtp_host

Required

false

Oozie Email Action SMTP Authentication Password

Description

SMTP password for Oozie email action

Related Name

oozie.email.smtp.password

Default Value

API Name

oozie_email_smtp_password

Required

false

Oozie Email Action SMTP Authentication Username

Description

SMTP username for Oozie email action

Related Name

oozie.email.smtp.username

Default Value

API Name

oozie_email_smtp_username

Required

false

Oozie Server Plugins

Description

Comma-separated list of Oozie plug-ins to be activated. If one plugin cannot be loaded, all the plugins are ignored.

Related Name

oozie.services.ext

Default Value

API Name

oozie_plugins_list

Required

false

Maximum concurrency for a given callable type

Description

Maximum concurrency for a given callable type.. Each command is a callable type: submit, start, run, etc.. Each action type is a callable type: MapReduce, SSH, sub-workflow, etc. All commands that use action executors (action-start, action-end. etc.) use the action type as the callable type.

Related Name

oozie.service.CallableQueueService.callable.concurrency

Default Value

10

API Name

oozie_service_callablequeueservice_callable_concurrency

Required

false

Maximum Callable Queue Size

Description

Maximum callable queue size

Related Name

oozie.service.CallableQueueService.queue.size

Default Value

10000

API Name

oozie_service_callablequeueservice_queue_size

Required

false

Number Threads For Executing Callables

Description

Number of threads used for executing callables

Related Name

oozie.service.CallableQueueService.threads

Default Value

50

API Name

oozie_service_callablequeueservice_threads

Required

false

Enable The Metrics Instrumentation Service

Description

Whether to use the Codehale-based metrics for instrumentation. Enabling this disables the 'instrumentation' REST endpoint and enables the 'metrics' REST endpoint (*hostname:port*/v2/admin/metrics).

Related Name

Default Value

true

API Name

oozie_use_metric_instrumentation

Required

false

Enable Oozie Server Web Console

Description

If true, enables the Oozie Server web console. ExtJS 2.2 zip archive must be extracted to /var/lib/oozie on the same host as the Oozie Server.

Related Name

Default Value

false

API Name

oozie_web_console

Required

false

Days to Keep Completed Bundle Jobs

Description

Completed bundle jobs older than this value, in days, will be purged by the PurgeService.

Related Name

oozie.service.PurgeService.bundle.older.than

Default Value

7 day(s)

API Name

purgeservice_bundle_older_than

Required

false

Days to Keep Completed Coordinator Jobs

Description

Completed coordinator jobs older than this value, in days, will be purged by the PurgeService.

Related Name

oozie.service.PurgeService.coord.older.than

Default Value

7 day(s)

API Name

purgeservice_coord_older_than

Required

false

Days to Keep Completed Workflow Jobs

Description

Completed workflow jobs older than this value, in days, will be purged by the PurgeService.

Related Name

oozie.service.PurgeService.older.than

Default Value

30 day(s)

API Name

purgeservice_older_than

Required

false

Enable Purge for Long-Running Coordinator Jobs

Description

Whether to purge completed workflows and their corresponding coordinator actions of long-running coordinator jobs if the completed workflow jobs are older than the value specified in oozie.service.PurgeService.older.than.

Related Name

oozie.service.PurgeService.purge.old.coord.action

Default Value

true

API Name

purgeservice_purge_old_coord_action

Required

false

Performance

Default Launcher Virtual CPU Cores

Description

The default number of Virtual CPU Cores that are allocated for the Launcher ApplicationMasters.

Related Name

oozie.launcher.default.vcores

Default Value

1

API Name

oozie_launcher_default_vcores

Required

false

Oozie Server Threadpool Size

Description

Controls the threadpool size for the Oozie Server (both Jetty and Tomcat).

Related Name

oozie.server.threadpool.max.threads

Default Value

150

API Name

oozie_service_threadpool_max_threads

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Oozie Email Action SMTP Port

Description

The SMTP server port to use for Oozie email action

Related Name

oozie.email.smtp.port

Default Value

25

API Name

oozie_email_smtp_prt

Required

false

Oozie HTTP Port

Description

Port of Oozie Server

Related Name

oozie.http.port

Default Value

11000

API Name

oozie_http_port

Required

false

Oozie HTTPS Port

Description

Port of the Oozie Server when using TLS/SSL.

Related Name

oozie.https.port

Default Value

11443

API Name

oozie_https_port

Required

false

Resource Management

Java Heap Size of Oozie Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

oozie_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Excluded Cipher Suites

Description

List of cipher suite names that should be excluded.

Related Name

oozie.https.exclude.cipher.suites

Default Value

TLS_ECDHE_RSA_WITH_RC4_128_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_WITH_RC4_128_MD5

API Name

oozie_https_exclude_cipher_suites

Required

false

Enabled TLS Protocols

Description

TLS protocols accepted by the Oozie Server.

Related Name

oozie.https.include.protocols

Default Value

SSLv2Hello, TLSv1, TLSv1.1, TLSv1.2

API Name

oozie_https_include_protocols

Required

false

Oozie TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Oozie is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

oozie.https.keystore.file

Default Value

/var/lib/oozie/.keystore

API Name

oozie_https_keystore_file

Required

false

Oozie TLS/SSL Server Keystore File Password

Description

The password for the Oozie keystore file.

Related Name

oozie.https.keystore.pass

Default Value

API Name

oozie_https_keystore_password

Required

false

Oozie TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Oozie might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

oozie.https.truststore.file

Default Value

API Name

oozie_https_truststore_file

Required

false

Oozie TLS/SSL Trust Store Password

Description

The password for the Oozie TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

oozie.https.truststore.pass

Default Value

API Name

oozie_https_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Oozie Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: Oozie Server Advanced Configuration Snippet (Safety Valve) for action-conf/default.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Advanced Configuration Snippet (Safety Valve) for action-conf/default.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_action_config_default_safety_valve

Required

true

Suppress Parameter Validation: Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_config_safety_valve

Required

true

Suppress Parameter Validation: Oozie Server Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_data_dir

Required

true

Suppress Parameter Validation: Oozie Database Connection Properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Database Connection Properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_connection_properties

Required

true

Suppress Parameter Validation: Oozie Server Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Database Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_host

Required

true

Suppress Parameter Validation: Oozie Server Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_name

Required

true

Suppress Parameter Validation: Oozie Server Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_password

Required

true

Suppress Parameter Validation: Oozie Server Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Database User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_user

Required

true

Suppress Parameter Validation: Oozie Datasource Properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Datasource Properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_datasource_properties

Required

true

Suppress Parameter Validation: Oozie Email Action From Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Email Action From Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_from_address

Required

true

Suppress Parameter Validation: Oozie Email Action SMTP Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Email Action SMTP Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_host

Required

true

Suppress Parameter Validation: Oozie Email Action SMTP Authentication Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Email Action SMTP Authentication Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_password

Required

true

Suppress Parameter Validation: Oozie Email Action SMTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Email Action SMTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_prt

Required

true

Suppress Parameter Validation: Oozie Email Action SMTP Authentication Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Email Action SMTP Authentication Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_username

Required

true

Suppress Parameter Validation: Oozie ActionService Executor Extension Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie ActionService Executor Extension Classes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_executor_extension_classes

Required

true

Suppress Parameter Validation: Oozie HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_http_port

Required

true

Suppress Parameter Validation: Excluded Cipher Suites

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Excluded Cipher Suites parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_exclude_cipher_suites

Required

true

Suppress Parameter Validation: Oozie TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_keystore_file

Required

true

Suppress Parameter Validation: Oozie TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_keystore_password

Required

true

Suppress Parameter Validation: Oozie HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_port

Required

true

Suppress Parameter Validation: Oozie TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_truststore_file

Required

true

Suppress Parameter Validation: Oozie TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_truststore_password

Required

true

Suppress Parameter Validation: Java Configuration Options for Oozie Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Oozie Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_java_opts

Required

true

Suppress Parameter Validation: Directory For JSP Temp Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Directory For JSP Temp Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_jsp_tmp_dir

Required

true

Suppress Parameter Validation: Default Launcher Queue

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Launcher Queue parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_launcher_default_queue

Required

true

Suppress Parameter Validation: Oozie Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_log_dir

Required

true

Suppress Parameter Validation: Oozie Server Plugins

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Plugins parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_plugins_list

Required

true

Suppress Parameter Validation: Oozie Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Oozie SchemaService Workflow Extension Schemas

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie SchemaService Workflow Extension Schemas parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_workflow_extension_schemas

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_audit_health

Required

true

Suppress Health Test: Callable Queue Size

Description

Whether to suppress the results of the Callable Queue Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_callablequeue_size_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_pause_duration

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_scm_health

Required

true

Suppress Health Test: Oozie Server Shared Library Check

Description

Whether to suppress the results of the Oozie Server Shared Library Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_shared_lib_version_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie_server_web_metric_collection

Required

true

Service-Wide

Advanced

Oozie Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

oozie_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

oozie

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

oozie

API Name

process_username

Required

true

Database

Database Dump File

Description

File where the database gets dumped to or loaded from.

Related Name

Default Value

/tmp/oozie_database_dump.zip

API Name

database_dump_file

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Oozie Server Monitoring Thresholds

Description

The health test thresholds of the overall Oozie Server health. The check returns "Concerning" health if the percentage of "Healthy" Oozie Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Oozie Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

oozie_servers_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "I F (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", " streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Hive Service

Description

Name of the Hive service that this Oozie service instance depends on. This is used to configure Oozie HCat integration.

Related Name

Default Value

API Name

hive_service

Required

false

MapReduce Service

Description

Service to run MapReduce jobs against

Related Name

Default Value

API Name

mapreduce_yarn_service

Required

true

Oozie Event Listeners

Description

List of event listeners used by the Oozie service. Listeners needed for JMS or SLA integration are automatically emitted if they are enabled.

Related Name

oozie.service.EventHandlerService.event.listeners

Default Value

API Name

oozie_event_listeners

Required

false

JMS Broker

Description

URL of the JMS Broker used by the Oozie service in JMS integration is enabled.

Related Name

oozie.jms.producer.connection.properties

Default Value

tcp://localhost:61616

API Name

oozie_jms_broker

Required

false

Oozie Load Balancer Hostname

Description

Hostname of the load balancer used if Oozie HA is enabled.

Related Name

Default Value

API Name

oozie_load_balancer

Required

false

Coordinator Job Lookup Interval

Description

Coordinator Job Lookup trigger command is scheduled at this interval (in seconds).

Related Name

oozie.service.CoordMaterializeTriggerService.lookup.interval

Default Value

5 minute(s)

API Name

oozie_service_coord_lookup_interval

Required

false

Coordinator Action Input Check Default Timeout

Description

Default timeout for a Coordinator Action input check (in minutes) for a Coordinator Job.

Related Name

oozie.service.coord.normal.default.timeout

Default Value

2 hour(s)

API Name

oozie_service_coord_normal_default_timeout

Required

false

ShareLib Root Directory

Description

Root of the directory in HDFS where the Oozie ShareLibs are stored. The libraries are stored in the share/lib subdirectory under the specified root directory.

Related Name

oozie.service.WorkflowAppService.system.libpath

Default Value

/user/oozie

API Name

oozie_sharelib_rootdir

Required

true

Oozie Upload ShareLib Command Timeout

Description

The timeout in seconds used for the Oozie Upload ShareLib command. When the value is zero, there is no timeout for the command.

Related Name

Default Value

270

API Name

oozie_upload_sharelib_cmd_timeout

Required

false

Oozie Upload ShareLib Command Concurrency Level

Description

The number of threads that Oozie will use for the Upload ShareLib command.

Related Name

Default Value

8

API Name

oozie_upload_sharelib_concurrency

Required

false

Enable JMS Integration

Description

Whether to configure Oozie properties needed for JMS integration

Related Name

Default Value

false

API Name

oozie_use_jms

Required

false

Enable SLA Integration

Description

Whether to configure Oozie properties needed for SLA integration

Related Name

Default Value

false

API Name

oozie_use_sla

Required

false

Use ACLs on Znode

Description

Use ACLs on Znode while a secure ZooKeeper is used for Oozie High Availability. Note: This config is not emitted if ZooKeeper is not secure.

Related Name

oozie.zookeeper.secure

Default Value

true

API Name

oozie_zk_secure

Required

false

ZooKeeper Namespace

Description

Namespace used by this Oozie service in ZooKeeper when High Availability is enabled.

Related Name

oozie.zookeeper.namespace

Default Value

oozie

API Name

oozie_zookeeper_namespace

Required

false

Spark on Yarn Service

Description

Name of the Spark on Yarn service that this Oozie service instance depends on

Related Name

Default Value

API Name

spark_on_yarn_service

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Oozie service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Ports and Addresses

Oozie Load Balancer HTTP Port

Description

HTTP port of the load balancer used if Oozie HA is enabled and SSL is disabled.

Related Name

Default Value

API Name

oozie_load_balancer_http_port

Required

false

Oozie Load Balancer HTTPS Port

Description

HTTPS port of the load balancer used if Oozie HA is enabled and SSL is enabled.

Related Name

Default Value

API Name

oozie_load_balancer_https_port

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

oozie

API Name

kerberos_princ_name

Required

true

Oozie Credential Classes

Description

A list of credential class mappings for CredentialsProvider.

Related Name

oozie.credentials.credentialclasses

Default Value

hcat=org.apache.oozie.action.hadoop.HCatCredentials
hbase=org.apache.oozie.action.hadoop.HbaseCredentials
hive2=org.apache.oozie.action.hadoop.Hive2Credentials

API Name

oozie_credential_classes

Required

false

Enable TLS/SSL for Oozie

Description

Encrypt communication between clients and Oozie using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

oozie.https.enabled

Default Value

false

API Name

oozie_use_ssl

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Oozie Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Oozie Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: Oozie Server Advanced Configuration Snippet (Safety Valve) for action-conf/default.xml

Description

Whether to suppress configuration warnings produced by the Oozie Server Advanced Configuration Snippet (Safety Valve) for action-conf/default.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_action_config_default_safety_valve

Required

true

Suppress Configuration Validator: Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml

Description

Whether to suppress configuration warnings produced by the Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_config_safety_valve

Required

true

Suppress Configuration Validator: Oozie Server Data Directory

Description

Whether to suppress configuration warnings produced by the Oozie Server Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_data_dir

Required

true

Suppress Configuration Validator: Oozie Database Connection Properties

Description

Whether to suppress configuration warnings produced by the Oozie Database Connection Properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_connection_properties

Required

true

Suppress Configuration Validator: Oozie Server Database Host

Description

Whether to suppress configuration warnings produced by the Oozie Server Database Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_host

Required

true

Suppress Configuration Validator: Oozie Server Database Name

Description

Whether to suppress configuration warnings produced by the Oozie Server Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_name

Required

true

Suppress Configuration Validator: Oozie Server Database Password

Description

Whether to suppress configuration warnings produced by the Oozie Server Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_password

Required

true

Suppress Configuration Validator: Oozie Server Database User

Description

Whether to suppress configuration warnings produced by the Oozie Server Database User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_database_user

Required

true

Suppress Configuration Validator: Oozie Datasource Properties

Description

Whether to suppress configuration warnings produced by the Oozie Datasource Properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_datasource_properties

Required

true

Suppress Configuration Validator: Oozie Email Action From Address

Description

Whether to suppress configuration warnings produced by the Oozie Email Action From Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_from_address

Required

true

Suppress Configuration Validator: Oozie Email Action SMTP Host

Description

Whether to suppress configuration warnings produced by the Oozie Email Action SMTP Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_host

Required

true

Suppress Configuration Validator: Oozie Email Action SMTP Authentication Password

Description

Whether to suppress configuration warnings produced by the Oozie Email Action SMTP Authentication Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_password

Required

true

Suppress Configuration Validator: Oozie Email Action SMTP Port

Description

Whether to suppress configuration warnings produced by the Oozie Email Action SMTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_prt

Required

true

Suppress Configuration Validator: Oozie Email Action SMTP Authentication Username

Description

Whether to suppress configuration warnings produced by the Oozie Email Action SMTP Authentication Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_email_smtp_username

Required

true

Suppress Configuration Validator: Oozie ActionService Executor Extension Classes

Description

Whether to suppress configuration warnings produced by the Oozie ActionService Executor Extension Classes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_executor_extension_classes

Required

true

Suppress Configuration Validator: Oozie HTTP Port

Description

Whether to suppress configuration warnings produced by the Oozie HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_http_port

Required

true

Suppress Configuration Validator: Excluded Cipher Suites

Description

Whether to suppress configuration warnings produced by the Excluded Cipher Suites configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_exclude_cipher_suites

Required

true

Suppress Configuration Validator: Oozie TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Oozie TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_keystore_file

Required

true

Suppress Configuration Validator: Oozie TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Oozie TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_keystore_password

Required

true

Suppress Configuration Validator: Oozie HTTPS Port

Description

Whether to suppress configuration warnings produced by the Oozie HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_port

Required

true

Suppress Configuration Validator: Oozie TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Oozie TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_truststore_file

Required

true

Suppress Configuration Validator: Oozie TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Oozie TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_https_truststore_password

Required

true

Suppress Configuration Validator: Java Configuration Options for Oozie Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Oozie Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_java_opts

Required

true

Suppress Configuration Validator: Directory For JSP Temp Files

Description

Whether to suppress configuration warnings produced by the Directory For JSP Temp Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_jsp_tmp_dir

Required

true

Suppress Configuration Validator: Default Launcher Queue

Description

Whether to suppress configuration warnings produced by the Default Launcher Queue configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_launcher_default_queue

Required

true

Suppress Configuration Validator: Oozie Server Log Directory

Description

Whether to suppress configuration warnings produced by the Oozie Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_log_dir

Required

true

Suppress Configuration Validator: Oozie Server Plugins

Description

Whether to suppress configuration warnings produced by the Oozie Server Plugins configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_plugins_list

Required

true

Suppress Configuration Validator: Oozie Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Oozie Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Oozie SchemaService Workflow Extension Schemas

Description

Whether to suppress configuration warnings produced by the Oozie SchemaService Workflow Extension Schemas configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oozie_workflow_extension_schemas

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Database Dump File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Dump File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_dump_file

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Oozie Credential Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Credential Classes parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_credential_classes

Required

true

Suppress Parameter Validation: Oozie Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_env_safety_valve

Required

true

Suppress Parameter Validation: Oozie Event Listeners

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Event Listeners parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_event_listeners

Required

true

Suppress Parameter Validation: JMS Broker

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMS Broker parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_jms_broker

Required

true

Suppress Parameter Validation: Oozie Load Balancer Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Load Balancer Hostname parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_load_balancer

Required

true

Suppress Parameter Validation: Oozie Load Balancer HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Load Balancer HTTP Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_load_balancer_http_port

Required

true

Suppress Parameter Validation: Oozie Load Balancer HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Load Balancer HTTPS Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_load_balancer_https_port

Required

true

Suppress Configuration Validator: Oozie Server Count Validator

Description

Whether to suppress configuration warnings produced by the Oozie Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_server_count_validator

Required

true

Suppress Parameter Validation: ShareLib Root Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ShareLib Root Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_sharelib_rootdir

Required

true

Suppress Parameter Validation: ZooKeeper Namespace

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Namespace parameter.

Related Name

Default Value

false

API Name

service_config_suppression_oozie_zookeeper_namespace

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Oozie Server Health

Description

Whether to suppress the results of the Oozie Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_oozie_oozie_servers_healthy

Required

true

Ozone Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/ozone

API Name

client_config_root_dir

Required

true

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-metrics2.properties

Description

For advanced use only, a string to be inserted into the client configuration for ozone-conf/hadoop-metrics2.properties.

Related Name

Default Value

API Name

ozone-conf/hadoop-metrics2.properties_client_config_safety_valve

Required

false

Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for ozone-conf/ozone-site.xml.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_client_config_safety_valve

Required

false

Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only, a string to be inserted into the client configuration for ozone-conf/ssl-client.xml.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_client_config_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Security

Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Gateway TLS/SSL Trust Store Password

Description

The password for the Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-metrics2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-metrics2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/hadoop-metrics2.properties_client_config_safety_valve

Required

true

Suppress Parameter Validation: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_client_config_safety_valve

Required

true

Suppress Parameter Validation: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

HttpFS Gateway

Advanced

HttpFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HTTPFS_GATEWAY_role_env_safety_valve

Required

false

HttpFS Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/httpfs-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/httpfs-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/httpfs-site.xml_role_safety_valve

Required

false

HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Logs

HttpFS Gateway Log Directory

Description

The log directory for log files of the role HttpFS Gateway.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

HttpFS Gateway Logging Threshold

Description

The minimum log level for HttpFS Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

HttpFS Gateway Maximum Log File Backups

Description

The maximum number of rolled log files to keep for HttpFS Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

HttpFS Gateway Max Log Size

Description

The maximum size, in megabytes, per log file for HttpFS Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

httpfs_gateway_fd_thresholds

Required

false

HttpFS Gateway Host Health Test

Description

When computing the overall HttpFS Gateway health, consider the host's health.

Related Name

Default Value

true

API Name

httpfs_gateway_host_health_enabled

Required

false

HttpFS Gateway Process Health Test

Description

Enables the health test that the HttpFS Gateway's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

httpfs_gateway_scm_health_enabled

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Hive Proxy User Groups for Ozone HttpFS

Description

Comma-delimited list of groups from which to allow the Hive user to impersonate others when connecting to Ozone HttpFS. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

httpfs.proxyuser.hive.groups

Default Value

*

API Name

httpfs.proxyuser.hive.groups

Required

true

Hive Proxy User Hosts for Ozone HttpFS

Description

Comma-delimited list of hosts from which to allow the Hive user to impersonate others when connecting to Ozone HttpFS. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

httpfs.proxyuser.hive.hosts

Default Value

*

API Name

httpfs.proxyuser.hive.hosts

Required

true

Hue Proxy User Groups for Ozone HttpFS

Description

Comma-delimited list of groups from which to allow the Hue user to impersonate others when connecting to Ozone HttpFS. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

httpfs.proxyuser.hue.groups

Default Value

*

API Name

httpfs.proxyuser.hue.groups

Required

true

Hue Proxy User Hosts for Ozone HttpFS

Description

Comma-delimited list of hosts from which to allow the Hue user to impersonate others when connecting to Ozone HttpFS. To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

httpfs.proxyuser.hue.hosts

Default Value

*

API Name

httpfs.proxyuser.hue.hosts

Required

true

Ozone HttpFS Gateway HTTP Bind Hostname

Description

The actual address the HttpFS Gateway web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.httpfs.http-address'.

Related Name

ozone.httpfs.http-bind-host

Default Value

0.0.0.0

API Name

ozone.httpfs.http-bind-host

Required

false

Java Heap Size of HttpFS Gateway

Description

Maximum size for the Java process heap memory.

Related Name

ozone_httpfs_gateway_max_heap_size

Default Value

1 GiB

API Name

ozone_httpfs_gateway_max_heap_size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Ozone HttpFS Gateway HTTP Web UI Port

Description

The base port that the HttpFS Gateway web user interface listens on. The host name of the HttpFS Gateway is combined with this port to form the 'ozone.httpfs.http-address'.

Related Name

ozone.httpfs.http-port

Default Value

9778

API Name

ozone.httpfs.http-port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the HttpFS Gateway roles.

Related Name

Default Value

httpfs

API Name

kerberos_role_princ_name

Required

true

HttpFS Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that HttpFS Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

HttpFS Gateway TLS/SSL Trust Store Password

Description

The password for the HttpFS Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for HttpFS Gateway

Description

Encrypt communication between clients and HttpFS Gateway using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

HttpFS Gateway TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when HttpFS Gateway is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

HttpFS Gateway TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when HttpFS Gateway is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

HttpFS Gateway TLS/SSL Server Keystore File Password

Description

The password for the HttpFS Gateway keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hive Proxy User Groups for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups for Ozone HttpFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hive.groups

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts for Ozone HttpFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hive.hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups for Ozone HttpFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hue.groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts for Ozone HttpFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hue.hosts

Required

true

Suppress Parameter Validation: HttpFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_gateway_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: HttpFS Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/httpfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/httpfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/httpfs-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone HttpFS Gateway HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone HttpFS Gateway HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.httpfs.http-bind-host

Required

true

Suppress Parameter Validation: Ozone HttpFS Gateway HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone HttpFS Gateway HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.httpfs.http-port

Required

true

Suppress Parameter Validation: Java Heap Size of HttpFS Gateway

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of HttpFS Gateway parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_httpfs_gateway_max_heap_size

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: HttpFS Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: HttpFS Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: HttpFS Gateway TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: HttpFS Gateway TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: HttpFS Gateway TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Gateway TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_httpfs_gateway_unexpected_exits

Required

true

Ozone DataNode

Advanced

Ozone DataNode Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-audit-log4j2.properties

Description

For advanced use only. A string to be inserted into ozone-conf/dn-audit-log4j2.properties for this role only.

Related Name

Default Value

API Name

ozone-conf/dn-audit-log4j2.properties_role_safety_valve

Required

false

Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-container-log4j2.properties

Description

For advanced use only. A string to be inserted into ozone-conf/dn-container-log4j2.properties for this role only.

Related Name

Default Value

API Name

ozone-conf/dn-container-log4j2.properties_role_safety_valve

Required

false

Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Ozone DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

OZONE_DATANODE_role_env_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Logs

Ozone DataNode Log Directory

Description

The log directory for log files of the role Ozone DataNode.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

Ozone DataNode Logging Threshold

Description

The minimum log level for Ozone DataNode logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ozone DataNode Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ozone DataNode logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ozone DataNode Max Log Size

Description

The maximum size, in megabytes, per log file for Ozone DataNode logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ozone_datanode_fd_thresholds

Required

false

Ozone DataNode Host Health Test

Description

When computing the overall Ozone DataNode health, consider the host's health.

Related Name

Default Value

true

API Name

ozone_datanode_host_health_enabled

Required

false

Ozone DataNode Process Health Test

Description

Enables the health test that the Ozone DataNode's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ozone_datanode_scm_health_enabled

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Datanode Ratis Metadata Directory

Description

One or more directories used for storing Datanode Ratis metadata. Ideally, this should be mapped to a fast disk like an SSD.

Related Name

dfs.container.ratis.datanode.storage.dir

Default Value

/var/lib/hadoop-ozone/datanode/ratis/data

API Name

dfs.container.ratis.datanode.storage.dir

Required

true

Number of Disks where Blocks are Stored that are Allowed to Fail

Description

The number of disks where blocks are stored that are allowed to fail before a datanode stops offering service. Set this property to -1 to specify that an unlimited number of disks can fail. If set to -1, there must be at least one good disk remaining on which to store blocks.

Related Name

failed.data.volumes.tolerated

Default Value

-1

API Name

failed.data.volumes.tolerated

Required

false

Number of Disks that Store Block Metadata that are Allowed to Fail

Description

The number of disks that store block metadata that are allowed to fail before a datanode stops offering service. Set this property to -1 to specify that an unlimited number of disks can fail. If set to -1, there must be at least one good disk remaining on which to store block metadata.

Related Name

failed.metadata.volumes.tolerated

Default Value

-1

API Name

failed.metadata.volumes.tolerated

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

2 minute(s)

API Name

graceful_stop_timeout

Required

false

Datanode Data Directory

Description

Determines where on the local filesystem HDDS data will be stored.

Related Name

hdds.datanode.dir

Default Value

/var/lib/hadoop-ozone/datanode/data

API Name

hdds.datanode.dir

Required

true

Datanode Out-Of-Service Replication Limit Factor

Description

Decommissioning and maintenance nodes can handle more replication commands than in-service nodes due to reduced load. This multiplier determines the increased queue capacity and executor pool size. The current default is 2.0

Related Name

hdds.datanode.replication.outofservice.limit.factor

Default Value

API Name

hdds.datanode.replication.outofservice.limit.factor

Required

false

Datanode Replication Streams Limit

Description

The maximum number of replication commands a single datanode can execute simultaneously. The current default is 10.

Related Name

hdds.datanode.replication.streams.limit

Default Value

API Name

hdds.datanode.replication.streams.limit

Required

false

Ozone Datanode HTTP Bind Hostname

Description

The actual address the Ozone Datanode web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.datanode.http-address'.

Related Name

ozone.datanode.http-bind-host

Default Value

0.0.0.0

API Name

ozone.datanode.http-bind-host

Required

false

Secure Ozone Datanode HTTPS Bind Hostname

Description

The actual address the Ozone Datanode web server will bind to using HTTPS. If this optional address is set, it overrides only the hostname portion of 'ozone.datanode.https-address'.

Related Name

ozone.datanode.https-bind-host

Default Value

0.0.0.0

API Name

ozone.datanode.https-bind-host

Required

false

HSTS Header for DataNode UI

Description

HSTS Header (Strict-Transport-Security) value to use

Related Name

ozone.http.header.Strict-Transport-Security

Default Value

max-age=63072000; includeSubDomains;

API Name

ozone.http.header.Strict-Transport-Security

Required

false

Datanode Metadata Directory

Description

Determines where on the local filesystem datanode security certificates will be stored.

Related Name

ozone.metadata.dirs

Default Value

/var/lib/hadoop-ozone/datanode/ozone-metadata

API Name

ozone.metadata.dirs

Required

true

Datanode ID Directory

Description

Ozone Datanode ID Directory

Related Name

ozone.scm.datanode.id.dir

Default Value

/var/lib/hadoop-ozone/datanode

API Name

ozone.scm.datanode.id.dir

Required

true

Java Heap Size of DataNode

Description

Maximum size for the Java process heap memory.

Related Name

ozone_datanode_heap_size

Default Value

4 GiB

API Name

ozone_datanode_heap_size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Datanode Ratis IPC Port for Admin Requests

Description

The container IPC port number for admin requests.

Related Name

dfs.container.ratis.admin.port

Default Value

9857

API Name

dfs.container.ratis.admin.port

Required

true

Datanode Ratis IPC Port for Server-to-Server Communication

Description

The container IPC port number for server-to-server communication.

Related Name

dfs.container.ratis.server.port

Default Value

9856

API Name

dfs.container.ratis.server.port

Required

true

Ozone Datanode HTTP Web UI Port

Description

The base port that the Ozone Datanode web user interface listens on. The host name is combined with this port to form the 'hdds.datanode.http-address'.

Related Name

ozone.datanode.http-port

Default Value

9882

API Name

ozone.datanode.http-port

Required

true

Ozone Datanode Port (TLS/SSL)

Description

The base port that the Ozone Datanode web user interface listens on when using HTTPS. The host name is combined with this port to form the 'hdds.datanode.https-address'.

Related Name

ozone.datanode.https-port

Default Value

9883

API Name

ozone.datanode.https-port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Ozone DataNode roles.

Related Name

Default Value

dn

API Name

kerberos_role_princ_name

Required

true

Ozone DataNode TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ozone DataNode might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Ozone DataNode TLS/SSL Trust Store Password

Description

The password for the Ozone DataNode TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ozone DataNode

Description

Encrypt communication between clients and Ozone DataNode using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ozone DataNode TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Ozone DataNode is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Ozone DataNode TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ozone DataNode is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Ozone DataNode TLS/SSL Server Keystore File Password

Description

The password for the Ozone DataNode keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Datanode Ratis IPC Port for Admin Requests

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Ratis IPC Port for Admin Requests parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.admin.port

Required

true

Suppress Parameter Validation: Datanode Ratis Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Ratis Metadata Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.datanode.storage.dir

Required

true

Suppress Parameter Validation: Datanode Ratis IPC Port for Server-to-Server Communication

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Ratis IPC Port for Server-to-Server Communication parameter.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.server.port

Required

true

Suppress Parameter Validation: Datanode Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.datanode.dir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Ozone DataNode Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ozone DataNode Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-audit-log4j2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/dn-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-container-log4j2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-container-log4j2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/dn-container-log4j2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Datanode HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Datanode HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.http-bind-host

Required

true

Suppress Parameter Validation: Ozone Datanode HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Datanode HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.http-port

Required

true

Suppress Parameter Validation: Secure Ozone Datanode HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Ozone Datanode HTTPS Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.https-bind-host

Required

true

Suppress Parameter Validation: Ozone Datanode Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Datanode Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.https-port

Required

true

Suppress Parameter Validation: HSTS Header for DataNode UI

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSTS Header for DataNode UI parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Parameter Validation: Datanode Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Metadata Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.metadata.dirs

Required

true

Suppress Parameter Validation: Datanode ID Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode ID Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.datanode.id.dir

Required

true

Suppress Parameter Validation: Java Heap Size of DataNode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of DataNode parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_datanode_heap_size

Required

true

Suppress Parameter Validation: Ozone DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_datanode_role_env_safety_valve

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ozone DataNode TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ozone DataNode TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ozone DataNode TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Ozone DataNode TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ozone DataNode TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone DataNode TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_datanode_unexpected_exits

Required

true

Ozone Manager

Advanced

Ozone Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/om-audit-log4j2.properties

Description

For advanced use only. A string to be inserted into ozone-conf/om-audit-log4j2.properties for this role only.

Related Name

Default Value

API Name

ozone-conf/om-audit-log4j2.properties_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-audit.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ranger-ozone-audit.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ranger-ozone-audit.xml_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ranger-ozone-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ranger-ozone-policymgr-ssl.xml_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-security.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ranger-ozone-security.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ranger-ozone-security.xml_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Ozone Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

OZONE_MANAGER_role_env_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Logs

Ozone Manager Log Directory

Description

The log directory for log files of the role Ozone Manager.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

Ozone Manager Logging Threshold

Description

The minimum log level for Ozone Manager logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ozone Manager Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ozone Manager logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ozone Manager Max Log Size

Description

The maximum size, in megabytes, per log file for Ozone Manager logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ozone_manager_fd_thresholds

Required

false

Ozone Manager Host Health Test

Description

When computing the overall Ozone Manager health, consider the host's health.

Related Name

Default Value

true

API Name

ozone_manager_host_health_enabled

Required

false

Ozone Manager Process Health Test

Description

Enables the health test that the Ozone Manager's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ozone_manager_scm_health_enabled

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

2 minute(s)

API Name

graceful_stop_timeout

Required

false

OM ID

Description

ID uniquely identifying each broker or controller. Never set this property at the group level; it should always be overridden on instance level.

Related Name

om.id

Default Value

API Name

om.id

Required

false

Java Heap Size of Ozone Manager

Description

Maximum size for the Java process heap memory.

Related Name

om_max_heap_size

Default Value

4 GiB

API Name

om_max_heap_size

Required

false

Ozone Default Bucket Layout

Description

This configuration controls the default bucket layout that the OM will use when creating a bucket if the client does not specify one. Supported values are OBJECT_STORE, FILE_SYSTEM_OPTIMIZED, and LEGACY.

Related Name

ozone.default.bucket.layout

Default Value

API Name

ozone.default.bucket.layout

Required

false

Ozone Filesystem Trash Checkpoint Interval

Description

Number of minutes between trash checkpoints

Related Name

ozone.fs.trash.checkpoint.interval

Default Value

1 hour(s)

API Name

ozone.fs.trash.checkpoint.interval

Required

false

Ozone Filesystem Trash Interval

Description

Controls the number of minutes after which a trash checkpoint directory is deleted permanently

Related Name

ozone.fs.trash.interval

Default Value

1 day(s)

API Name

ozone.fs.trash.interval

Required

false

HSTS Header for Ozone Manager UI

Description

HSTS Header (Strict-Transport-Security) value to use

Related Name

ozone.http.header.Strict-Transport-Security

Default Value

max-age=63072000; includeSubDomains;

API Name

ozone.http.header.Strict-Transport-Security

Required

false

Ozone Manager Metadata Directory

Description

Determines where on the local filesystem Ozone Manager security certificates will be stored.

Related Name

ozone.metadata.dirs

Default Value

/var/lib/hadoop-ozone/om/ozone-metadata

API Name

ozone.metadata.dirs

Required

true

Ozone Manager Data Directory

Description

Directory where the OzoneManager stores its metadata.

Related Name

ozone.om.db.dirs

Default Value

/var/lib/hadoop-ozone/om/data

API Name

ozone.om.db.dirs

Required

true

Ozone Manager HTTP Bind Hostname

Description

The actual address the OM web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.om.http-address'.

Related Name

ozone.om.http-bind-host

Default Value

0.0.0.0

API Name

ozone.om.http-bind-host

Required

false

Secure Ozone Manager HTTPS Bind Hostname

Description

The actual address the OM web server will bind to using HTTPS. If this optional address is set, it overrides only the hostname portion of 'ozone.om.https-address'.

Related Name

ozone.om.https-bind-host

Default Value

0.0.0.0

API Name

ozone.om.https-bind-host

Required

false

Enable Ozone S3 Multi-Tenancy feature

Description

Enable Ozone S3 Multi-Tenancy feature in Ozone Manager. This feature requires Kerberos Authentication to be enabled.

Related Name

ozone.om.multitenancy.enabled

Default Value

false

API Name

ozone.om.multitenancy.enabled

Required

false

New Ozone Manager Nodes

Description

Hostnames of newly added ozone manager nodes. If more than one hostname is to be added then put a ',' between hostnames, e.g, [hostname1,hostname2,hostname3]'.

Related Name

ozone.om.new.added.nodes

Default Value

API Name

ozone.om.new.added.nodes

Required

false

Ozone Manager Ratis Storage Directory

Description

This directory is used for storing Ozone Manager's Ratis metadata like logs. Ideally, this should be mapped to a fast disk like an SSD.

Related Name

ozone.om.ratis.storage.dir

Default Value

/var/lib/hadoop-ozone/om/ratis

API Name

ozone.om.ratis.storage.dir

Required

true

Ozone Server Replication Factor

Description

The default value of the replication factor for objects. The default is used if replication is not specified when creating a key or if no default replication is set at the bucket. Supported values for RATIS are 1, 3. Supported values for EC are rs-3-2-1024k, rs-6-3-1024k, rs-10-4-1024k, XOR-3-2-1024k, XOR-6-3-1024k, XOR-10-4-4096K (i.e XOR-3-2-{CHUNK_SIZE})

Related Name

ozone.server.default.replication

Default Value

3

API Name

ozone.server.default.replication

Required

true

Ozone Server Replication Type

Description

The default replication type to be used for Objects. The default is used when a type is not specified when creating an Object or no default value is set for the bucket. Supported values are RATIS, STAND_ALONE, and EC.

Related Name

ozone.server.default.replication.type

Default Value

RATIS

API Name

ozone.server.default.replication.type

Required

true

Ozone Manager Upgrade Need Finalization Canary Enabled

Description

Determines if the Ozone Manager Upgrade Need Finalization Canary is enabled.

Related Name

ozone_om_upgrade_need_finalization_canary_enabled

Default Value

true

API Name

ozone_om_upgrade_need_finalization_canary_enabled

Required

false

Ozone Manager Upgrade Need Finalization Canary Timeout

Description

Sets Ozone Manager Upgrade Need Finalization Canary's timeout.

Related Name

ozone_om_upgrade_need_finalization_canary_timeout

Default Value

30 second(s)

API Name

ozone_om_upgrade_need_finalization_canary_timeout

Required

false

Ranger Ozone Plugin Conf Path

Description

Staging directory for Ranger Ozone Plugin Configuration. This should generally not be changed.

Related Name

ranger_ozone_plugin_conf_path

Default Value

/etc/ranger/ozone-plugin

API Name

ranger_ozone_plugin_conf_path

Required

true

Ranger Ozone Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.ozone.policy.cache.dir

Default Value

/var/lib/ranger/ozone/policy-cache

API Name

ranger_ozone_plugin_policy_cache_directory

Required

true

Ranger Ozone Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/hadoop-ozone/ranger-audit/solr/spool

API Name

ranger_ozone_plugin_solr_audit_spool_directory

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Ozone Manager HTTP Web UI Port

Description

The base port that the Ozone Manager HTTP web user interface listens on. The host name of the Ozone Manager is combined with this port to form the 'ozone.om.http-address'.

Related Name

ozone.om.http-port

Default Value

9874

API Name

ozone.om.http-port

Required

true

Secure Ozone Manager Web UI Port (TLS/SSL)

Description

The base port that the Ozone Manager HTTP web user interface listens on when using HTTPS. The host name of the Ozone Manager is combined with this port to form the 'ozone.om.https-address'.

Related Name

ozone.om.https-port

Default Value

9875

API Name

ozone.om.https-port

Required

false

Ozone Manager Ratis port

Description

The base port that Ozone Manager's Ratis Server listens on if multiple Ozone Manager's are configured.

Related Name

ozone.om.ratis-port

Default Value

9872

API Name

ozone.om.ratis-port

Required

false

Ozone Manager RPC port

Description

The base port that Ozone Manager listens on when serving RPCs. The host name of the Ozone Manager is combined with this port to form the 'ozone.om.address'.

Related Name

ozone.om.rpc-port

Default Value

9862

API Name

ozone.om.rpc-port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the

value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Ozone Manager roles.

Related Name

Default Value

om

API Name

kerberos_role_princ_name

Required

true

Ozone Manager TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ozone Manager might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Ozone Manager TLS/SSL Trust Store Password

Description

The password for the Ozone Manager TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ozone Manager

Description

Encrypt communication between clients and Ozone Manager using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ozone Manager TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Ozone Manager is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Ozone Manager TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ozone Manager is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Ozone Manager TLS/SSL Server Keystore File Password

Description

The password for the Ozone Manager keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user

with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Ozone Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: OM ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OM ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_om.id

Required

true

Suppress Parameter Validation: Java Heap Size of Ozone Manager

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of Ozone Manager parameter.

Related Name

Default Value

false

API Name

role_config_suppression_om_max_heap_size

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/om-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/om-audit-log4j2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/om-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HSTS Header for Ozone Manager UI

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSTS Header for Ozone Manager UI parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Parameter Validation: Ozone Manager Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Metadata Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.metadata.dirs

Required

true

Suppress Parameter Validation: Ozone Manager Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.db.dirs

Required

true

Suppress Parameter Validation: Ozone Manager HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.http-bind-host

Required

true

Suppress Parameter Validation: Ozone Manager HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.http-port

Required

true

Suppress Parameter Validation: Secure Ozone Manager HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Ozone Manager HTTPS Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.https-bind-host

Required

true

Suppress Parameter Validation: Secure Ozone Manager Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Ozone Manager Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.https-port

Required

true

Suppress Parameter Validation: New Ozone Manager Nodes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the New Ozone Manager Nodes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.new.added.nodes

Required

true

Suppress Parameter Validation: Ozone Manager Ratis port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Ratis port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.ratis-port

Required

true

Suppress Parameter Validation: Ozone Manager Ratis Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Ratis Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.ratis.storage.dir

Required

true

Suppress Parameter Validation: Ozone Manager RPC port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager RPC port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.rpc-port

Required

true

Suppress Parameter Validation: Ozone Server Replication Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Server Replication Factor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.server.default.replication

Required

true

Suppress Parameter Validation: Ozone Server Replication Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Server Replication Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.server.default.replication.type

Required

true

Suppress Parameter Validation: Ozone Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_manager_role_env_safety_valve

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Ozone Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Ozone Plugin Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_conf_path

Required

true

Suppress Parameter Validation: Ranger Ozone Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Ozone Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Ozone Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Ozone Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ozone Manager TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ozone Manager TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ozone Manager TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Ozone Manager TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ozone Manager TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Manager TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Ozone Manager Upgrade Need Finalization Canary

Description

Whether to suppress the results of the Ozone Manager Upgrade Need Finalization Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_om_upgrade_need_finalization_canary

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_manager_unexpected_exits

Required

true

Ozone Prometheus

Advanced

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-prometheus.yml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-prometheus.yml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-prometheus.yml_role_safety_valve

Required

false

Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/prometheus-token

Description

For advanced use only. A string to be inserted into ozone-conf/prometheus-token for this role only.

Related Name

Default Value

API Name

ozone-conf/prometheus-token_role_safety_valve

Required

false

Ozone Prometheus Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

OZONE_PROMETHEUS_role_env_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Logs

Ozone Prometheus Log Directory

Description

The log directory for log files of the role Ozone Prometheus.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ozone_prometheus_fd_thresholds

Required

false

Ozone Prometheus Host Health Test

Description

When computing the overall Ozone Prometheus health, consider the host's health.

Related Name

Default Value

true

API Name

ozone_prometheus_host_health_enabled

Required

false

Ozone Prometheus Process Health Test

Description

Enables the health test that the Ozone Prometheus's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ozone_prometheus_scm_health_enabled

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

CA File Path

Description

Location of the CA File for Prometheus

Related Name

ozone.prometheus.ca.file

Default Value

AUTO_TLS_CA_FILE

API Name

ozone.prometheus.ca.file

Required

false

Prometheus Data Retention time.

Description

How long to retain samples in storage. Units Supported: y, w, d, h, m, s, ms.

Related Name

ozone.prometheus.data.retention.time

Default Value

15d

API Name

ozone.prometheus.data.retention.time

Required

false

Prometheus Data Directory

Description

Directory where the Prometheus Server stores its metadata.

Related Name

ozone.prometheus.db.dir

Default Value

/var/lib/hadoop-ozone/prometheus/data

API Name

ozone.prometheus.db.dir

Required

true

Prometheus server extra flags.

Description

Extra command line flags that can be used while starting up the server. For example, '--query.timeout=2m --query.max-samples=5000'

Related Name

ozone.prometheus.extra.flags

Default Value

API Name

ozone.prometheus.extra.flags

Required

false

Prometheus server log level.

Description

Only log messages with the given severity or above. One of: [debug, info, warn, error]

Related Name

ozone.prometheus.log.level

Default Value

info

API Name

ozone.prometheus.log.level

Required

false

Prometheus Binary Location

Description

Location of the unarchived Prometheus binary.

Related Name

prometheus.location

Default Value

API Name

prometheus.location

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Prometheus HTTP Port

Description

The base port that the prometheus web user interface listens on.

Related Name

ozone.prometheus.http-port

Default Value

9094

API Name

ozone.prometheus.http-port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ozone Prometheus Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Prometheus Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-prometheus.yml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-prometheus.yml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-prometheus.yml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/prometheus-token

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/prometheus-token parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/prometheus-token_role_safety_valve

Required

true

Suppress Parameter Validation: CA File Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the CA File Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.ca.file

Required

true

Suppress Parameter Validation: Prometheus Data Retention time.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Data Retention time. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.data.retention.time

Required

true

Suppress Parameter Validation: Prometheus Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.db.dir

Required

true

Suppress Parameter Validation: Prometheus server extra flags.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus server extra flags. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.extra.flags

Required

true

Suppress Parameter Validation: Prometheus HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.http-port

Required

true

Suppress Parameter Validation: Prometheus server log level.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus server log level. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.log.level

Required

true

Suppress Parameter Validation: Ozone Prometheus Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Prometheus Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_prometheus_role_env_safety_valve

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Prometheus Binary Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Binary Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus.location

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_prometheus_unexpected_exits

Required

true

Ozone Recon

Advanced

Ozone Recon Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Ozone Recon Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

OZONE_RECON_role_env_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Logs

Ozone Recon Log Directory

Description

The log directory for log files of the role Ozone Recon.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

Ozone Recon Logging Threshold

Description

The minimum log level for Ozone Recon logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ozone Recon Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ozone Recon logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ozone Recon Max Log Size

Description

The maximum size, in megabytes, per log file for Ozone Recon logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ozone_recon_fd_thresholds

Required

false

Ozone Recon Host Health Test

Description

When computing the overall Ozone Recon health, consider the host's health.

Related Name

Default Value

true

API Name

ozone_recon_host_health_enabled

Required

false

Ozone Recon Process Health Test

Description

Enables the health test that the Ozone Recon's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ozone_recon_scm_health_enabled

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HSTS Header for Recon UI

Description

HSTS Header (Strict-Transport-Security) value to use

Related Name

ozone.http.header.Strict-Transport-Security

Default Value

max-age=63072000; includeSubDomains;

API Name

ozone.http.header.Strict-Transport-Security

Required

false

Recon Metadata Directory

Description

Determines where on the local filesystem recon security certificates will be stored.

Related Name

ozone.metadata.dirs

Default Value

/var/lib/hadoop-ozone/recon/ozone-metadata

API Name

ozone.metadata.dirs

Required

true

Recon Data Directory

Description

Directory where the Recon Server stores its metadata.

Related Name

ozone.recon.db.dir

Default Value

/var/lib/hadoop-ozone/recon/data

API Name

ozone.recon.db.dir

Required

true

Enable HeatMap Feature in Recon

Description

Enables HeatMap Feature in Recon.

Related Name

ozone.recon.heatmap.enable

Default Value

true

API Name

ozone.recon.heatmap.enable

Required

false

Recon HTTP Bind Hostname

Description

The actual address the Recon web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.recon.http-address'.

Related Name

ozone.recon.http-bind-host

Default Value

0.0.0.0

API Name

ozone.recon.http-bind-host

Required

false

Secure Recon HTTPS Bind Hostname

Description

The actual address the Recon web server will bind to using HTTPS. If this optional address is set, it overrides only the hostname portion of 'ozone.recon.https-address'.

Related Name

ozone.recon.https-bind-host

Default Value

0.0.0.0

API Name

ozone.recon.https-bind-host

Required

false

Recon OzoneManager Data Directory

Description

Directory where the Recon Server stores OzoneManager's metadata

Related Name

ozone.recon.om.db.dir

Default Value

/var/lib/hadoop-ozone/recon/om/data

API Name

ozone.recon.om.db.dir

Required

true

Recon StorageContainerManager Data Directory

Description

Directory where the Recon Server stores StorageContainerManager's metadata

Related Name

ozone.recon.scm.db.dirs

Default Value

/var/lib/hadoop-ozone/recon/scm/data

API Name

ozone.recon.scm.db.dirs

Required

true

Java Heap Size of Recon

Description

Maximum size for the Java process heap memory.

Related Name

ozone_recon_max_heap_size

Default Value

1 GiB

API Name

ozone_recon_max_heap_size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Recon HTTP Web UI Port

Description

The base port that the Recon web user interface listens on. The host name of the Recon web user interface is combined with this port to form the 'ozone.recon.http-address'.

Related Name

ozone.recon.http-port

Default Value

9888

API Name

ozone.recon.http-port

Required

true

Secure Recon Web UI Port (TLS/SSL)

Description

The base port that the Recon web user interface listens on when using HTTPS. The host name of the Recon web user interface is combined with this port to form the 'ozone.recon.https-address'.

Related Name

ozone.recon.https-port

Default Value

9889

API Name

ozone.recon.https-port

Required

false

Recon RPC Port

Description

The base port that Recon listens on when serving RPCs. The host name of Recon is combined with this port to form the 'ozone.recon.address'.

Related Name

ozone.recon.rpc-port

Default Value

9891

API Name

ozone.recon.rpc-port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Ozone Recon roles.

Related Name

Default Value

recon

API Name

kerberos_role_princ_name

Required

true

Ozone Recon TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ozone Recon might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Ozone Recon TLS/SSL Trust Store Password

Description

The password for the Ozone Recon TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ozone Recon

Description

Encrypt communication between clients and Ozone Recon using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ozone Recon TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Ozone Recon is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Ozone Recon TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ozone Recon is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Ozone Recon TLS/SSL Server Keystore File Password

Description

The password for the Ozone Recon keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Ozone Recon Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ozone Recon Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HSTS Header for Recon UI

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSTS Header for Recon UI parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Parameter Validation: Recon Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon Metadata Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.metadata.dirs

Required

true

Suppress Parameter Validation: Recon Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.db.dir

Required

true

Suppress Parameter Validation: Recon HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.http-bind-host

Required

true

Suppress Parameter Validation: Recon HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.http-port

Required

true

Suppress Parameter Validation: Secure Recon HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Recon HTTPS Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.https-bind-host

Required

true

Suppress Parameter Validation: Secure Recon Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Recon Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.https-port

Required

true

Suppress Parameter Validation: Recon OzoneManager Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon OzoneManager Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.om.db.dir

Required

true

Suppress Parameter Validation: Recon RPC Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon RPC Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.rpc-port

Required

true

Suppress Parameter Validation: Recon StorageContainerManager Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Recon StorageContainerManager Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.scm.db.dirs

Required

true

Suppress Parameter Validation: Java Heap Size of Recon

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of Recon parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_recon_max_heap_size

Required

true

Suppress Parameter Validation: Ozone Recon Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_recon_role_env_safety_valve

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ozone Recon TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ozone Recon TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ozone Recon TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Ozone Recon TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ozone Recon TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Recon TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_ozone_recon_unexpected_exits

Required

true

S3 Gateway

Advanced

S3 Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/s3g-audit-log4j2.properties

Description

For advanced use only. A string to be inserted into ozone-conf/s3g-audit-log4j2.properties for this role only.

Related Name

Default Value

API Name

ozone-conf/s3g-audit-log4j2.properties_role_safety_valve

Required

false

S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

S3 Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

S3_GATEWAY_role_env_safety_valve

Required

false

Logs

S3 Gateway Log Directory

Description

The log directory for log files of the role S3 Gateway.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

S3 Gateway Logging Threshold

Description

The minimum log level for S3 Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

S3 Gateway Maximum Log File Backups

Description

The maximum number of rolled log files to keep for S3 Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

S3 Gateway Max Log Size

Description

The maximum size, in megabytes, per log file for S3 Gateway logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

s3_gateway_fd_thresholds

Required

false

S3 Gateway Host Health Test

Description

When computing the overall S3 Gateway health, consider the host's health.

Related Name

Default Value

true

API Name

s3_gateway_host_health_enabled

Required

false

S3 Gateway Process Health Test

Description

Enables the health test that the S3 Gateway's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

s3_gateway_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

HSTS Header for S3G HTTPS Endpoint

Description

HSTS Header (Strict-Transport-Security) value to use

Related Name

ozone.http.header.Strict-Transport-Security

Default Value

max-age=63072000; includeSubDomains;

API Name

ozone.http.header.Strict-Transport-Security

Required

false

Ozone S3 Gateway HTTP Bind Hostname

Description

The actual address the S3 Gateway web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.s3g.http-address'.

Related Name

ozone.s3g.http-bind-host

Default Value

0.0.0.0

API Name

ozone.s3g.http-bind-host

Required

false

Secure Ozone S3 Gateway HTTPS Bind Hostname

Description

The actual address the S3 Gateway web server will bind to using HTTPS. If this optional address is set, it overrides only the hostname portion of 'ozone.s3g.https-address'.

Related Name

ozone.s3g.https-bind-host

Default Value

0.0.0.0

API Name

ozone.s3g.https-bind-host

Required

false

Java Heap Size of S3 Gateway

Description

Maximum size for the Java process heap memory.

Related Name

ozone_S3_gateway_max_heap_size

Default Value

1 GiB

API Name

ozone_S3_gateway_max_heap_size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Ozone S3 Gateway HTTP Web UI Port

Description

The base port that the S3 Gateway web user interface listens on. The host name of the S3 Gateway is combined with this port to form the 'ozone.s3g.http-address'.

Related Name

ozone.s3g.http-port

Default Value

9878

API Name

ozone.s3g.http-port

Required

true

Secure Ozone S3 Gateway Web UI Port (TLS/SSL)

Description

The base port that the S3 Gateway web user interface listens on when using HTTPS. The host name of the S3 Gateway is combined with this port to form the 'ozone.s3g.https-address'.

Related Name

ozone.s3g.https-port

Default Value

9879

API Name

ozone.s3g.https-port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the S3 Gateway roles.

Related Name

Default Value

s3g

API Name

kerberos_role_princ_name

Required

true

S3 Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that S3 Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

S3 Gateway TLS/SSL Trust Store Password

Description

The password for the S3 Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for S3 Gateway

Description

Encrypt communication between clients and S3 Gateway using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

S3 Gateway TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when S3 Gateway is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

S3 Gateway TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when S3 Gateway is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

S3 Gateway TLS/SSL Server Keystore File Password

Description

The password for the S3 Gateway keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: S3 Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: S3 Gateway Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/s3g-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/s3g-audit-log4j2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/s3g-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HSTS Header for S3G HTTPS Endpoint

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSTS Header for S3G HTTPS Endpoint parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Parameter Validation: Ozone S3 Gateway HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone S3 Gateway HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.http-bind-host

Required

true

Suppress Parameter Validation: Ozone S3 Gateway HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone S3 Gateway HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.http-port

Required

true

Suppress Parameter Validation: Secure Ozone S3 Gateway HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Ozone S3 Gateway HTTPS Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.https-bind-host

Required

true

Suppress Parameter Validation: Secure Ozone S3 Gateway Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Ozone S3 Gateway Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.https-port

Required

true

Suppress Parameter Validation: Java Heap Size of S3 Gateway

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of S3 Gateway parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_s3_gateway_max_heap_size

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: S3 Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_s3_gateway_role_env_safety_valve

Required

true

Suppress Parameter Validation: S3 Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: S3 Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: S3 Gateway TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: S3 Gateway TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: S3 Gateway TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Gateway TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_s3_gateway_unexpected_exits

Required

true

Service-Wide

Advanced

Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only, a string to be inserted into ozone-conf/ozone-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_service_safety_valve

Required

false

Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only, a string to be inserted into ozone-conf/ssl-client.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_service_safety_valve

Required

false

Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only, a string to be inserted into ozone-conf/ssl-server.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_service_safety_valve

Required

false

Ozone Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

OZONE_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ozone DataNode Monitoring Thresholds

Description

The health test thresholds of the overall Ozone DataNode health. The check returns "Concerning" health if the percentage of "Healthy" Ozone DataNodes falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ozone DataNodes falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 90.0 %

API Name

OZONE_OZONE_DATANODE_healthy_thresholds

Required

false

Healthy Ozone Manager Monitoring Thresholds

Description

The health test thresholds of the overall Ozone Manager health. The check returns "Concerning" health if the percentage of "Healthy" Ozone Managers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ozone Managers falls below the critical threshold.

Related Name

Default Value

Warning: 75.0 %, Critical: 50.0 %

API Name

OZONE_OZONE_MANAGER_healthy_thresholds

Required

false

Healthy Storage Container Manager Monitoring Thresholds

Description

The health test thresholds of the overall Storage Container Manager health. The check returns "Concerning" health if the percentage of "Healthy" Storage Container Managers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Storage Container Managers falls below the critical threshold.

Related Name

Default Value

Warning: 75.0 %, Critical: 50.0 %

API Name

OZONE_STORAGE_CONTAINER_MANAGER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

CM API Bucket Owner

Description

Name of the role to use to get credentials for the kerberos principal to set the owner when creating a bucket via CM APIs. If no role name is specified, the Hive kerberos principal is used by default.

Related Name

cm.api.bucket.owner

Default Value

API Name

cm.api.bucket.owner

Required

false

Ozone HttpFS Gateway Proxy User Groups

Description

Comma-delimited list of groups to allow the Ozone HttpFS Gateway to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.httpfs.groups

Default Value

*

API Name

hadoop.proxyuser.httpfs.groups

Required

true

Ozone HttpFS Gateway Proxy User Hosts

Description

Comma-delimited list of hosts to allow the Ozone HttpFS Gateway to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.httpfs.hosts

Default Value

*

API Name

hadoop.proxyuser.httpfs.hosts

Required

true

Hue Proxy User Groups

Description

Comma-delimited list of groups to allow the Hue user to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.hue.groups

Default Value

*

API Name

hadoop.proxyuser.hue.groups

Required

true

Hue Proxy User Hosts

Description

Comma-delimited list of hosts to allow the Hue user to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.hue.hosts

Default Value

*

API Name

hadoop.proxyuser.hue.hosts

Required

true

Ozone Proxy User Groups

Description

Comma-delimited list of groups to allow the Ozone user to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.om.groups

Default Value

*

API Name

hadoop.proxyuser.om.groups

Required

true

Ozone Proxy User Hosts

Description

Comma-delimited list of hosts to allow the Ozone user to impersonate.To disable entirely, use a string that does not correspond to a group name, such as '_no_group_

Related Name

hadoop.proxyuser.om.hosts

Default Value

*

API Name

hadoop.proxyuser.om.hosts

Required

true

Choose RocksDB profile

Description

This property allows user to pick a configuration that tunes the RocksDB settings for the hardware it is running on. Right now, we have SSD and DISK as profile options.

Related Name

hdds.db.profile

Default Value

DISK

API Name

hdds.db.profile

Required

false

Enable HDDS gRPC Server TLS

Description

Enable HDDS gRPC server TLS on this cluster. Please note this won't take effect unless Kerberos Authentication (ozone.security.enabled) is enabled as well.

Related Name

hdds.grpc.tls.enabled

Default Value

false

API Name

hdds.grpc.tls.enabled

Required

false

Ozone Prometheus Endpoint Token

Description

Enables token based authentication for Prometheus servlet endpoints. This will disable SPNEGO based authentication on the endpoints.

Related Name

hdds.prometheus.endpoint.token

Default Value

API Name

hdds.prometheus.endpoint.token

Required

false

HDFS Service

Description

Name of the HDFS service that this Ozone service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

Ozone Administrators

Description

A comma separated list of Kerberos principals of Ozone Administrators. This will be effective only when security is enabled.

Related Name

ozone.administrators

Default Value

API Name

ozone.administrators

Required

false

Ozone Replication Factor

Description

Default replication factor value for keys stored in Ozone. The actual number of replications can be specified when writing the key. The default is used if replication value is not specified. Supported values: 1 and 3.

Related Name

ozone.replication

Default Value

3

API Name

ozone.replication

Required

true

Ozone Incremental Replication Extra Snapshots to Keep

Description

How many extra snapshots to keep that have been created by incremental Ozone replication on source and target clusters. By using the default value (0) only the snapshot from the latest incremental replication will be kept.

Related Name

ozone.replication.incremental.snapshots.keep

Default Value

0

API Name

ozone.replication.incremental.snapshots.keep

Required

false

Ozone SCM Primordial Node ID

Description

SCM Primordial Node ID is the hostname of the SCM which should act as a Root Certificate Authority(CA) for Ozone during security initialization. It is mandatory to have a Primordial Node ID when there is more than one SCM instance configured.

Related Name

ozone.scm.primordial.node.id

Default Value

API Name

ozone.scm.primordial.node.id

Required

false

Ozone SCM Service ID

Description

A final alphanumerical name to identify this Ozone service. The value is configured during installation, and should not be modified after that, as any change in the service id may cause service disruption.

Related Name

ozone.scm.service.id

Default Value

scm1

API Name

ozone.scm.service.id

Required

true

Enable Kerberos Authentication

Description

Enables Kerberos authentication for Ozone.

Related Name

ozone.security.enabled

Default Value

false

API Name

ozone.security.enabled

Required

false

Enable Kerberos Authentication for HTTP web consoles

Description

Enables Kerberos authentication for Ozone HTTP web consoles for all roles of this service using the SPNEGO protocol. Note: This is effective only if Kerberos is enabled for the Ozone service.

Related Name

ozone.security.http.kerberos.enabled

Default Value

false

API Name

ozone.security.http.kerberos.enabled

Required

false

Ozone Service ID

Description

A final alphanumerical name to identify this Ozone service. The value is configured during installation, and should not be modified after that, as any change in the service id may cause service disruption.

Related Name

ozone.service.id

Default Value

API Name

ozone.service.id

Required

true

Ozone Basic Health Check Enabled

Description

Determines if the Ozone Basic health check is enabled.

Related Name

ozone_basic_health_check_enabled

Default Value

true

API Name

ozone_basic_health_check_enabled

Required

false

Ozone Basic Health Check's Keystore's Key Encryption Algorithm

Description

Ozone Basic Health Check's Keystore's Key Encryption Algorithm

Related Name

ozone_basic_health_check_keystore_key_encryption_algo

Default Value

AES

API Name

ozone_basic_health_check_keystore_key_encryption_algo

Required

false

Ozone Basic Health Check's Keystore Type

Description

Ozone Basic Health Check's Keystore Type

Related Name

ozone_basic_health_check_keystore_type

Default Value

JCEKS

API Name

ozone_basic_health_check_keystore_type

Required

false

Ozone Basic Health Check's Timeout

Description

Ozone Basic Health Check's Timeout

Related Name

ozone_basic_health_check_timeout

Default Value

1 minute(s)

API Name

ozone_basic_health_check_timeout

Required

false

Ozone Java Options

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags would be passed here.

Related Name

ozone_java_opts

Default Value

java_args

API Name

ozone_java_opts

Required

false

Ranger Ozone Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_ozone_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/ozone

API Name

ranger_ozone_plugin_hdfs_audit_directory

Required

false

RANGER Service

Description

Name of the RANGER service that this Ozone service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Solr Service

Description

Name of the Solr service that this Ozone service instance depends on

Related Name

Default Value

API Name

solr_service

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Datanode Ratis IPC Port for Admin Requests

Description

Whether to suppress configuration warnings produced by the Datanode Ratis IPC Port for Admin Requests configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.admin.port

Required

true

Suppress Configuration Validator: Datanode Ratis Metadata Directory

Description

Whether to suppress configuration warnings produced by the Datanode Ratis Metadata Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.datanode.storage.dir

Required

true

Suppress Configuration Validator: Datanode Ratis IPC Port for Server-to-Server Communication

Description

Whether to suppress configuration warnings produced by the Datanode Ratis IPC Port for Server-to-Server Communication configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_dfs.container.ratis.server.port

Required

true

Suppress Configuration Validator: Balancing Interval

Description

Whether to suppress configuration warnings produced by the Balancing Interval configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.balancing.iteration.interval

Required

true

Suppress Configuration Validator: Exclude Containers from Balancing

Description

Whether to suppress configuration warnings produced by the Exclude Containers from Balancing configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.exclude.containers

Required

true

Suppress Configuration Validator: Exclude Datanodes

Description

Whether to suppress configuration warnings produced by the Exclude Datanodes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.exclude.datanodes

Required

true

Suppress Configuration Validator: Include Datanodes

Description

Whether to suppress configuration warnings produced by the Include Datanodes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.include.datanodes

Required

true

Suppress Configuration Validator: Container Move Replication Timeout

Description

Whether to suppress configuration warnings produced by the Container Move Replication Timeout configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.move.replication.timeout

Required

true

Suppress Configuration Validator: Container Move Timeout

Description

Whether to suppress configuration warnings produced by the Container Move Timeout configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.move.timeout

Required

true

Suppress Configuration Validator: Maximum Size Entering Target

Description

Whether to suppress configuration warnings produced by the Maximum Size Entering Target configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.entering.target.max

Required

true

Suppress Configuration Validator: Maximum Size Leaving Source

Description

Whether to suppress configuration warnings produced by the Maximum Size Leaving Source configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.leaving.source.max

Required

true

Suppress Configuration Validator: Maximum Size to Move in Balancing

Description

Whether to suppress configuration warnings produced by the Maximum Size to Move in Balancing configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.moved.max.per.iteration

Required

true

Suppress Configuration Validator: Datanode Data Directory

Description

Whether to suppress configuration warnings produced by the Datanode Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.datanode.dir

Required

true

Suppress Configuration Validator: Over Replication Processing Interval

Description

Whether to suppress configuration warnings produced by the Over Replication Processing Interval configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.over.replicated.interval

Required

true

Suppress Configuration Validator: Replication Thread Interval

Description

Whether to suppress configuration warnings produced by the Replication Thread Interval configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.thread.interval

Required

true

Suppress Configuration Validator: Under Replication Processing Interval

Description

Whether to suppress configuration warnings produced by the Under Replication Processing Interval configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.under.replicated.interval

Required

true

Suppress Configuration Validator: Datanode Container Protocol ACL

Description

Whether to suppress configuration warnings produced by the Datanode Container Protocol ACL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.security.client.datanode.container.protocol.acl

Required

true

Suppress Configuration Validator: SCM Client Certificate Protocol ACL

Description

Whether to suppress configuration warnings produced by the SCM Client Certificate Protocol ACL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.security.client.scm.certificate.protocol.acl

Required

true

Suppress Configuration Validator: Hive Proxy User Groups for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Groups for Ozone HttpFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hive.groups

Required

true

Suppress Configuration Validator: Hive Proxy User Hosts for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Hosts for Ozone HttpFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hive.hosts

Required

true

Suppress Configuration Validator: Hue Proxy User Groups for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Groups for Ozone HttpFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hue.groups

Required

true

Suppress Configuration Validator: Hue Proxy User Hosts for Ozone HttpFS

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Hosts for Ozone HttpFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs.proxyuser.hue.hosts

Required

true

Suppress Configuration Validator: HttpFS Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the HttpFS Gateway Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_httpfs_gateway_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the Role-Specific Kerberos Principal configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Configuration Validator: Storage Container Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Log Directory

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Topology Script File Name

Description

Whether to suppress configuration warnings produced by the Topology Script File Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_net.topology.script.file.name

Required

true

Suppress Configuration Validator: OM ID

Description

Whether to suppress configuration warnings produced by the OM ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_om.id

Required

true

Suppress Configuration Validator: Java Heap Size of Ozone Manager

Description

Whether to suppress configuration warnings produced by the Java Heap Size of Ozone Manager configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_om_max_heap_size

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-audit-log4j2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/dn-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-container-log4j2.properties

Description

Whether to suppress configuration warnings produced by the Ozone DataNode Advanced Configuration Snippet (Safety Valve) for ozone-conf/dn-container-log4j2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/dn-container-log4j2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-metrics2.properties

Description

Whether to suppress configuration warnings produced by the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-metrics2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/hadoop-metrics2.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-policy.xml

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-policy.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/hadoop-policy.xml_role_safety_valve

Required

true

Suppress Configuration Validator: HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/httpfs-site.xml

Description

Whether to suppress configuration warnings produced by the HttpFS Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/httpfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/httpfs-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/om-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/om-audit-log4j2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/om-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-prometheus.yml

Description

Whether to suppress configuration warnings produced by the Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-prometheus.yml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-prometheus.yml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/prometheus-token

Description

Whether to suppress configuration warnings produced by the Ozone Prometheus Advanced Configuration Snippet (Safety Valve) for ozone-conf/prometheus-token configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/prometheus-token_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-audit.xml

Description

Whether to suppress configuration warnings produced by the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-security.xml

Description

Whether to suppress configuration warnings produced by the Ozone Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ranger-ozone-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ranger-ozone-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/s3g-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the S3 Gateway Advanced Configuration Snippet (Safety Valve) for ozone-conf/s3g-audit-log4j2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/s3g-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/scm-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/scm-audit-log4j2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/scm-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the Ozone Client Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ozone Datanode HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Ozone Datanode HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.http-bind-host

Required

true

Suppress Configuration Validator: Ozone Datanode HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Ozone Datanode HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.http-port

Required

true

Suppress Configuration Validator: Secure Ozone Datanode HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the Secure Ozone Datanode HTTPS Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.https-bind-host

Required

true

Suppress Configuration Validator: Ozone Datanode Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Ozone Datanode Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.datanode.https-port

Required

true

Suppress Configuration Validator: HSTS Header for Ozone SCM UI

Description

Whether to suppress configuration warnings produced by the HSTS Header for Ozone SCM UI configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Configuration Validator: Ozone HttpFS Gateway HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Ozone HttpFS Gateway HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.httpfs.http-bind-host

Required

true

Suppress Configuration Validator: Ozone HttpFS Gateway HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Ozone HttpFS Gateway HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.httpfs.http-port

Required

true

Suppress Configuration Validator: Storage Container Manager Metadata Directory

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Metadata Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.metadata.dirs

Required

true

Suppress Configuration Validator: Ozone Manager Data Directory

Description

Whether to suppress configuration warnings produced by the Ozone Manager Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.db.dirs

Required

true

Suppress Configuration Validator: Ozone Manager HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Ozone Manager HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.http-bind-host

Required

true

Suppress Configuration Validator: Ozone Manager HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Ozone Manager HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.http-port

Required

true

Suppress Configuration Validator: Secure Ozone Manager HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the Secure Ozone Manager HTTPS Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.https-bind-host

Required

true

Suppress Configuration Validator: Secure Ozone Manager Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure Ozone Manager Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.https-port

Required

true

Suppress Configuration Validator: New Ozone Manager Nodes

Description

Whether to suppress configuration warnings produced by the New Ozone Manager Nodes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.new.added.nodes

Required

true

Suppress Configuration Validator: Ozone Manager Ratis port

Description

Whether to suppress configuration warnings produced by the Ozone Manager Ratis port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.ratis-port

Required

true

Suppress Configuration Validator: Ozone Manager Ratis Storage Directory

Description

Whether to suppress configuration warnings produced by the Ozone Manager Ratis Storage Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.ratis.storage.dir

Required

true

Suppress Configuration Validator: Ozone Manager RPC port

Description

Whether to suppress configuration warnings produced by the Ozone Manager RPC port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.om.rpc-port

Required

true

Suppress Configuration Validator: CA File Path

Description

Whether to suppress configuration warnings produced by the CA File Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.ca.file

Required

true

Suppress Configuration Validator: Prometheus Data Retention time.

Description

Whether to suppress configuration warnings produced by the Prometheus Data Retention time. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.data.retention.time

Required

true

Suppress Configuration Validator: Prometheus Data Directory

Description

Whether to suppress configuration warnings produced by the Prometheus Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.db.dir

Required

true

Suppress Configuration Validator: Prometheus server extra flags.

Description

Whether to suppress configuration warnings produced by the Prometheus server extra flags. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.extra.flags

Required

true

Suppress Configuration Validator: Prometheus HTTP Port

Description

Whether to suppress configuration warnings produced by the Prometheus HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.http-port

Required

true

Suppress Configuration Validator: Prometheus server log level.

Description

Whether to suppress configuration warnings produced by the Prometheus server log level. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.prometheus.log.level

Required

true

Suppress Configuration Validator: Recon Data Directory

Description

Whether to suppress configuration warnings produced by the Recon Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.db.dir

Required

true

Suppress Configuration Validator: Recon HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Recon HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.http-bind-host

Required

true

Suppress Configuration Validator: Recon HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Recon HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.http-port

Required

true

Suppress Configuration Validator: Secure Recon HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the Secure Recon HTTPS Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.https-bind-host

Required

true

Suppress Configuration Validator: Secure Recon Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure Recon Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.https-port

Required

true

Suppress Configuration Validator: Recon OzoneManager Data Directory

Description

Whether to suppress configuration warnings produced by the Recon OzoneManager Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.om.db.dir

Required

true

Suppress Configuration Validator: Recon RPC Port

Description

Whether to suppress configuration warnings produced by the Recon RPC Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.rpc-port

Required

true

Suppress Configuration Validator: Recon StorageContainerManager Data Directory

Description

Whether to suppress configuration warnings produced by the Recon StorageContainerManager Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.recon.scm.db.dirs

Required

true

Suppress Configuration Validator: Ozone S3 Gateway HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Ozone S3 Gateway HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.http-bind-host

Required

true

Suppress Configuration Validator: Ozone S3 Gateway HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Ozone S3 Gateway HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.http-port

Required

true

Suppress Configuration Validator: Secure Ozone S3 Gateway HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the Secure Ozone S3 Gateway HTTPS Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.https-bind-host

Required

true

Suppress Configuration Validator: Secure Ozone S3 Gateway Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure Ozone S3 Gateway Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.s3g.https-port

Required

true

Suppress Configuration Validator: Storage Container Manager Block Client port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Block Client port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.block.client.port

Required

true

Suppress Configuration Validator: Storage Container Manager Client port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Client port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.client.port

Required

true

Suppress Configuration Validator: Datanode ID Directory

Description

Whether to suppress configuration warnings produced by the Datanode ID Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.datanode.id.dir

Required

true

Suppress Configuration Validator: Storage Container Manager Datanode port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Datanode port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.datanode.port

Required

true

Suppress Configuration Validator: Storage Container Manager Data Directory

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.db.dirs

Required

true

Suppress Configuration Validator: Storage Container Manager GRPC port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager GRPC port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.grpc.port

Required

true

Suppress Configuration Validator: Storage Container Manager Ratis Storage Directory

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Ratis Storage Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.ha.ratis.storage.dir

Required

true

Suppress Configuration Validator: Storage Container Manager HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the Storage Container Manager HTTP Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.http-bind-host

Required

true

Suppress Configuration Validator: Storage Container Manager HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager HTTP Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.http-port

Required

true

Suppress Configuration Validator: Secure Storage Container Manager HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the Secure Storage Container Manager HTTPS Bind Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.https-bind-host

Required

true

Suppress Configuration Validator: Secure Storage Container Manager Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the Secure Storage Container Manager Web UI Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.https-port

Required

true

Suppress Configuration Validator: Storage Container Manager Ratis port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Ratis port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.ratis.port

Required

true

Suppress Configuration Validator: Storage Container Manager Security Service port

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Security Service port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.security.service.port

Required

true

Suppress Configuration Validator: Ozone Server Replication Factor

Description

Whether to suppress configuration warnings produced by the Ozone Server Replication Factor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.server.default.replication

Required

true

Suppress Configuration Validator: Ozone Server Replication Type

Description

Whether to suppress configuration warnings produced by the Ozone Server Replication Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.server.default.replication.type

Required

true

Suppress Configuration Validator: Java Heap Size of DataNode

Description

Whether to suppress configuration warnings produced by the Java Heap Size of DataNode configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_datanode_heap_size

Required

true

Suppress Configuration Validator: Ozone DataNode Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ozone DataNode Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_datanode_role_env_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of HttpFS Gateway

Description

Whether to suppress configuration warnings produced by the Java Heap Size of HttpFS Gateway configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_httpfs_gateway_max_heap_size

Required

true

Suppress Configuration Validator: Ozone Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ozone Manager Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_manager_role_env_safety_valve

Required

true

Suppress Configuration Validator: Ozone Prometheus Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ozone Prometheus Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_prometheus_role_env_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of Recon

Description

Whether to suppress configuration warnings produced by the Java Heap Size of Recon configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_recon_max_heap_size

Required

true

Suppress Configuration Validator: Ozone Recon Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ozone Recon Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_recon_role_env_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of S3 Gateway

Description

Whether to suppress configuration warnings produced by the Java Heap Size of S3 Gateway configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ozone_s3_gateway_max_heap_size

Required

true

Suppress Configuration Validator: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the Role Specific System Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Configuration Validator: Role Specific System User

Description

Whether to suppress configuration warnings produced by the Role Specific System User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Configuration Validator: Prometheus Binary Location

Description

Whether to suppress configuration warnings produced by the Prometheus Binary Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus.location

Required

true

Suppress Configuration Validator: Ranger Ozone Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Ozone Plugin Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_conf_path

Required

true

Suppress Configuration Validator: Ranger Ozone Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Ozone Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Ozone Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Ozone Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ozone_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: S3 Gateway Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the S3 Gateway Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_s3_gateway_role_env_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of Storage Container Manager

Description

Whether to suppress configuration warnings produced by the Java Heap Size of Storage Container Manager configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_scm_max_heap_size

Required

true

Suppress Configuration Validator: Storage Container Manager TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Storage Container Manager TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Storage Container Manager TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Storage Container Manager TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Storage Container Manager TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Storage Container Manager TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Storage Container Manager TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Storage Container Manager TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Storage Container Manager TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Storage Container Manager TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Storage Container Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_storage_container_manager_role_env_safety_valve

Required

true

Suppress Parameter Validation: CM API Bucket Owner

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the CM API Bucket Owner parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cm.api.bucket.owner

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Ozone HttpFS Gateway Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone HttpFS Gateway Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.httpfs.groups

Required

true

Suppress Parameter Validation: Ozone HttpFS Gateway Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone HttpFS Gateway Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.httpfs.hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.hue.groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.hue.hosts

Required

true

Suppress Parameter Validation: Ozone Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.om.groups

Required

true

Suppress Parameter Validation: Ozone Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop.proxyuser.om.hosts

Required

true

Suppress Parameter Validation: Ozone Prometheus Endpoint Token

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Prometheus Endpoint Token parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdds.prometheus.endpoint.token

Required

true

Suppress Configuration Validator: HttpFS Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the HttpFS Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_httpfs_gateway_count_validator

Required

true

Suppress Parameter Validation: Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone-conf/ozone-site.xml_service_safety_valve

Required

true

Suppress Parameter Validation: Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone-conf/ssl-client.xml_service_safety_valve

Required

true

Suppress Parameter Validation: Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone-conf/ssl-server.xml_service_safety_valve

Required

true

Suppress Parameter Validation: Ozone Administrators

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Administrators parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone.administrators

Required

true

Suppress Parameter Validation: Ozone SCM Primordial Node ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone SCM Primordial Node ID parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone.scm.primordial.node.id

Required

true

Suppress Parameter Validation: Ozone SCM Service ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone SCM Service ID parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone.scm.service.id

Required

true

Suppress Parameter Validation: Ozone Service ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Service ID parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone.service.id

Required

true

Suppress Parameter Validation: Ozone Basic Health Check's Keystore's Key Encryption Algorithm

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Basic Health Check's Keystore's Key Encryption Algorithm parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_basic_health_check_keystore_key_encryption_algo

Required

true

Suppress Parameter Validation: Ozone Basic Health Check's Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Basic Health Check's Keystore Type parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_basic_health_check_keystore_type

Required

true

Suppress Configuration Validator: Ozone DataNode Count Validator

Description

Whether to suppress configuration warnings produced by the Ozone DataNode Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_datanode_count_validator

Required

true

Suppress Parameter Validation: Ozone Java Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Java Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_java_opts

Required

true

Suppress Configuration Validator: Ozone Manager Count Validator

Description

Whether to suppress configuration warnings produced by the Ozone Manager Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_manager_count_validator

Required

true

Suppress Configuration Validator: Ozone Prometheus Count Validator

Description

Whether to suppress configuration warnings produced by the Ozone Prometheus Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_prometheus_count_validator

Required

true

Suppress Configuration Validator: Ozone Recon Count Validator

Description

Whether to suppress configuration warnings produced by the Ozone Recon Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_recon_count_validator

Required

true

Suppress Parameter Validation: Ozone Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ozone Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ozone_service_env_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Ozone Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Ozone Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_ozone_plugin_hdfs_audit_directory

Required

true

Suppress Configuration Validator: S3 Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the S3 Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_s3_gateway_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Configuration Validator: Storage Container Manager Count Validator

Description

Whether to suppress configuration warnings produced by the Storage Container Manager Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_storage_container_manager_count_validator

Required

true

Suppress Health Test: Ozone Basic Canary

Description

Whether to suppress the results of the Ozone Basic Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ozone_basic_health_check

Required

true

Suppress Health Test: Ozone DataNode Health

Description

Whether to suppress the results of the Ozone DataNode Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ozone_ozone_datanode_healthy

Required

true

Suppress Health Test: Ozone Manager Health

Description

Whether to suppress the results of the Ozone Manager Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ozone_ozone_manager_healthy

Required

true

Suppress Health Test: Storage Container Manager Health

Description

Whether to suppress the results of the Storage Container Manager Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ozone_storage_container_manager_healthy

Required

true

Storage Container Manager

Advanced

Storage Container Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-policy.xml

Description

For advanced use only. A string to be inserted into ozone-conf/hadoop-policy.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/hadoop-policy.xml_role_safety_valve

Required

false

Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ozone-site.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ozone-site.xml_role_safety_valve

Required

false

Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/scm-audit-log4j2.properties

Description

For advanced use only. A string to be inserted into ozone-conf/scm-audit-log4j2.properties for this role only.

Related Name

Default Value

API Name

ozone-conf/scm-audit-log4j2.properties_role_safety_valve

Required

false

Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-client.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-client.xml_role_safety_valve

Required

false

Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

For advanced use only. A string to be inserted into ozone-conf/ssl-server.xml for this role only.

Related Name

Default Value

API Name

ozone-conf/ssl-server.xml_role_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Role Specific System Group

Description

The group that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Role Specific System User

Description

The user that this role's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Storage Container Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STORAGE_CONTAINER_MANAGER_role_env_safety_valve

Required

false

Logs

Storage Container Manager Log Directory

Description

The log directory for log files of the role Storage Container Manager.

Related Name

log.dir

Default Value

/var/log/hadoop-ozone

API Name

log_dir

Required

false

Storage Container Manager Logging Threshold

Description

The minimum log level for Storage Container Manager logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Storage Container Manager Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Storage Container Manager logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Storage Container Manager Max Log Size

Description

The maximum size, in megabytes, per log file for Storage Container Manager logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

storage_container_manager_fd_thresholds

Required

false

Storage Container Manager Host Health Test

Description

When computing the overall Storage Container Manager health, consider the host's health.

Related Name

Default Value

true

API Name

storage_container_manager_host_health_enabled

Required

false

Storage Container Manager Process Health Test

Description

Enables the health test that the Storage Container Manager's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

storage_container_manager_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

2 minute(s)

API Name

graceful_stop_timeout

Required

false

Balancing Interval

Description

The interval period between each iteration of Container Balancer. The current default is 70m. This means that Container Balancer will balance every 70 minutes. Units supported: d, h, m, s, ms.

Related Name

hdds.container.balancer.balancing.iteration.interval

Default Value

API Name

hdds.container.balancer.balancing.iteration.interval

Required

false

Maximum Percentage of Datanodes Involved in Balancing

Description

Maximum percentage of healthy, in-service datanodes that can be involved in balancing in one iteration (for example, '20' for 20%).

Related Name

hdds.container.balancer.datanodes.involved.max.percentage.per.iteration

Default Value

20

API Name

hdds.container.balancer.datanodes.involved.max.percentage.per.iteration

Required

false

Exclude Containers from Balancing

Description

Containers to exclude from balancing. Specified as a string of Container IDs (for example, '1, 2, 3').

Related Name

hdds.container.balancer.exclude.containers

Default Value

API Name

hdds.container.balancer.exclude.containers

Required

false

Exclude Datanodes

Description

A comma separated string of Datanode hostnames or IP addresses that will be excluded from balancing.

Related Name

hdds.container.balancer.exclude.datanodes

Default Value

API Name

hdds.container.balancer.exclude.datanodes

Required

false

Include Datanodes

Description

A comma separated string of Datanode hostnames or IP addresses that will be the only participants in balancing.

Related Name

hdds.container.balancer.include.datanodes

Default Value

API Name

hdds.container.balancer.include.datanodes

Required

false

Number of Balancing Iterations

Description

Number of iterations that Container Balancer will run for.

Related Name

hdds.container.balancer.iterations

Default Value

10

API Name

hdds.container.balancer.iterations

Required

false

Container Move Replication Timeout

Description

The amount of time to allow a single container's replication from source to target as part of container move. The current default is 50m. This means that if "hdds.container.balancer.move.timeout" is 65m, then out of those 65 minutes 50 minutes will be the deadline for replication to complete. The value of this configuration should always be less than "hdds.container.balancer.move.timeout". Units supported: d, h, m, s, ms.

Related Name

hdds.container.balancer.move.replication.timeout

Default Value

API Name

hdds.container.balancer.move.replication.timeout

Required

false

Container Move Timeout

Description

The amount of time to allow a single container to move from source to target. The current default is 65m. This means that a container is allowed a total of 65 minutes to complete its move from a source Datanode to a target Datanode, as part of container balancing. Units supported: d, h, m, s, ms.

Related Name

hdds.container.balancer.move.timeout

Default Value

API Name

hdds.container.balancer.move.timeout

Required

false

Maximum Size Entering Target

Description

The maximum size that can enter a target datanode in each iteration while balancing. This is the sum of data from multiple sources. Units supported: eb, pb, tb, gb, mb, kb, b.

Related Name

hdds.container.balancer.size.entering.target.max

Default Value

26gb

API Name

hdds.container.balancer.size.entering.target.max

Required

false

Maximum Size Leaving Source

Description

The maximum size that can leave a source datanode in each iteration while balancing. This is the sum of data moving to multiple targets. Units supported: eb, pb, tb, gb, mb, kb, b.

Related Name

hdds.container.balancer.size.leaving.source.max

Default Value

26gb

API Name

hdds.container.balancer.size.leaving.source.max

Required

false

Maximum Size to Move in Balancing

Description

The maximum size of data that will be moved by Container Balancer in one iteration. Units supported: eb, pb, tb, gb, mb, kb, b.

Related Name

hdds.container.balancer.size.moved.max.per.iteration

Default Value

500gb

API Name

hdds.container.balancer.size.moved.max.per.iteration

Required

false

Balancing Threshold

Description

The percentage deviation from average utilization, after which a node will be rebalanced (for example, '10' for 10%).

Related Name

hdds.container.balancer.utilization.threshold

Default Value

10.0

API Name

hdds.container.balancer.utilization.threshold

Required

false

Datanode Delete Container Limit

Description

A limit to restrict the total number of delete container commands queued on a datanode.

Related Name

hdds.scm.replication.datanode.delete.container.limit

Default Value

API Name

hdds.scm.replication.datanode.delete.container.limit

Required

false

Datanode Reconstruction Weight

Description

When counting the number of replication commands on a datanode, the number of reconstruction commands is multiplied by this weight to ensure reconstruction commands use more of the "hdds.scm.replication.datanode.replication.limit" capacity, as they are more expensive to process. The current default is 3.

Related Name

hdds.scm.replication.datanode.reconstruction.weight

Default Value

API Name

hdds.scm.replication.datanode.reconstruction.weight

Required

false

Datanode Replication Limit

Description

A limit to restrict the total number of replication and reconstruction commands queued on a datanode. The current default is 20.

Related Name

hdds.scm.replication.datanode.replication.limit

Default Value

API Name

hdds.scm.replication.datanode.replication.limit

Required

false

Inflight Limit Factor

Description

The overall replication task limit on a cluster is the number of healthy nodes, times the "hdds.scm.replication.datanode.replication.limit". This factor, which should be from zero through 1, scales that limit down to reduce the overall number of replicas pending creation on the cluster. A setting of zero disables global limit checking. A setting of 1 effectively disables it, by making the limit equal to the above equation. The current default is 0.75.

Related Name

hdds.scm.replication.inflight.limit.factor

Default Value

API Name

hdds.scm.replication.inflight.limit.factor

Required

false

Remaining Redundancy For Maintenance

Description

The number of redundant container replicas which must be available for a node to enter maintenance. If putting a node into maintenance reduces the redundancy below this value, the node will remain in the ENTERING_MAINTENANCE state until a new replica is created. For an EC container, redundancy is 1 if there are a total of data + 1 replicas, meaning 1 more replica can be lost before this container becomes unrecoverable. Example configurations: Consider an EC(3-2) container. If the value of this configuration is 1, then 1 Datanode hosting its replica can be put into maintenance and 4 other replicas should be available. If the value is 0, then 2 Datanodes hosting its replicas can be put into maintenance and 3 other replicas should be available. Set this to a high value to be safer but require more time for nodes to enter maintenance. The current default is 1.

Related Name

hdds.scm.replication.maintenance.remaining.redundancy

Default Value

API Name

hdds.scm.replication.maintenance.remaining.redundancy

Required

false

Over Replication Processing Interval

Description

How frequently to check if there is work to process on the over replicated queue. The current default is 30s. This means that every 30 seconds, this thread will process over replicated containers identified by Replication Manager. Units supported: d, h, m, s, ms.

Related Name

hdds.scm.replication.over.replicated.interval

Default Value

API Name

hdds.scm.replication.over.replicated.interval

Required

false

Replication Thread Interval

Description

There is a replication monitor thread running inside SCM which takes care of replicating the containers in the cluster. This property is used to configure the interval in which that thread runs. The current default is 300s. This means that the replication thread will run every 300 seconds. Units supported: d, h, m, s, ms.

Related Name

hdds.scm.replication.thread.interval

Default Value

API Name

hdds.scm.replication.thread.interval

Required

false

Under Replication Processing Interval

Description

How frequently to check if there is work to process on the under replicated queue. The current default is 30s. This means that every 30 seconds, this thread will process under replicated containers identified by Replication Manager. Units supported: d, h, m, s, ms.

Related Name

hdds.scm.replication.under.replicated.interval

Default Value

API Name

hdds.scm.replication.under.replicated.interval

Required

false

Datanode Container Protocol ACL

Description

ACLs that define which users can access the Datanode Container Protocol in SCM. It is a comma separated list of Kerberos Principals.

Related Name

hdds.security.client.datanode.container.protocol.acl

Default Value

OZONE_SERVICE_PRINCIPALS

API Name

hdds.security.client.datanode.container.protocol.acl

Required

false

SCM Client Certificate Protocol ACL

Description

ACLs that define which users can access the SCM Certificate Protocol. It is a comma separated list of Kerberos Principals.

Related Name

hdds.security.client.scm.certificate.protocol.acl

Default Value

OZONE_ADMINS, OZONE_SERVICE_PRINCIPALS

API Name

hdds.security.client.scm.certificate.protocol.acl

Required

false

Topology Script File Name

Description

Full path to a custom topology script on the host file system. The topology script is used to determine the rack location of nodes. If left with "{{DEFAULT_TOPOLOGY_SCRIPT}}", a topology script will be provided that uses your hosts' rack information, visible in the "Hosts" page.

Related Name

net.topology.script.file.name

Default Value

DEFAULT_TOPOLOGY_SCRIPT

API Name

net.topology.script.file.name

Required

false

HSTS Header for Ozone SCM UI

Description

HSTS Header (Strict-Transport-Security) value to use

Related Name

ozone.http.header.Strict-Transport-Security

Default Value

max-age=63072000; includeSubDomains;

API Name

ozone.http.header.Strict-Transport-Security

Required

false

Storage Container Manager Metadata Directory

Description

Determines where on the local filesystem SCM security certificates will be stored.

Related Name

ozone.metadata.dirs

Default Value

/var/lib/hadoop-ozone/scm/ozone-metadata

API Name

ozone.metadata.dirs

Required

true

Storage Container Manager Data Directory

Description

Directory where the StorageContainerManager stores its metadata

Related Name

ozone.scm.db.dirs

Default Value

/var/lib/hadoop-ozone/scm/data

API Name

ozone.scm.db.dirs

Required

true

Storage Container Manager Ratis Storage Directory

Description

Storage directory used by SCM to write Ratis logs.

Related Name

ozone.scm.ha.ratis.storage.dir

Default Value

/var/lib/hadoop-ozone/scm/ratis

API Name

ozone.scm.ha.ratis.storage.dir

Required

true

Storage Container Manager HTTP Bind Hostname

Description

The actual address the SCM web server will bind to. If this optional address is set, it overrides only the hostname portion of 'ozone.scm.http-address'.

Related Name

ozone.scm.http-bind-host

Default Value

0.0.0.0

API Name

ozone.scm.http-bind-host

Required

false

Secure Storage Container Manager HTTPS Bind Hostname

Description

The actual address the SCM web server will bind to using HTTPS. If this optional address is set, it overrides only the hostname portion of 'ozone.scm.https-address'.

Related Name

ozone.scm.https-bind-host

Default Value

0.0.0.0

API Name

ozone.scm.https-bind-host

Required

false

Pipeline Per Volume Factor

Description

Non negative number that scales the number of Erasure Coding pipelines per Erasure Coding scheme. The maximum number of pipelines will be limited to the number of healthy volumes in the cluster divided by the number of nodes required for the EC scheme, multiplied by this factor. The current default is 1.

Related Name

ozone.scm.pipeline.per.volume.factor

Default Value

API Name

ozone.scm.pipeline.per.volume.factor

Required

false

Ozone Storage Container Manager Safemode Canary Enabled

Description

Determines if the Ozone Storage Container Manager Safemode checker canary is enabled.

Related Name

ozone_scm_safemode_canary_enabled

Default Value

true

API Name

ozone_scm_safemode_canary_enabled

Required

false

Ozone Storage Container Manager Safemode Canary Timeout

Description

Ozone Storage Container Manager Safemode Canary's timeout

Related Name

ozone_scm_safemode_canary_timeout

Default Value

30 second(s)

API Name

ozone_scm_safemode_canary_timeout

Required

false

Ozone Storage Container Manager Upgrade Need Finalization Canary Enabled

Description

Determines if the Ozone Storage Container Manager Upgrade Need Finalization Canary is enabled.

Related Name

ozone_scm_upgrade_need_finalization_canary_enabled

Default Value

true

API Name

ozone_scm_upgrade_need_finalization_canary_enabled

Required

false

Ozone Storage Container Manager Upgrade Need Finalization Canary Timeout

Description

Sets Ozone Storage Container Manager Upgrade Need Finalization Canary's timeout.

Related Name

ozone_scm_upgrade_need_finalization_canary_timeout

Default Value

30 second(s)

API Name

ozone_scm_upgrade_need_finalization_canary_timeout

Required

false

Java Heap Size of Storage Container Manager

Description

Maximum size for the Java process heap memory.

Related Name

scm_max_heap_size

Default Value

4 GiB

API Name

scm_max_heap_size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Storage Container Manager Block Client port

Description

The port number of the Ozone SCM block client service.

Related Name

ozone.scm.block.client.port

Default Value

9863

API Name

ozone.scm.block.client.port

Required

false

Storage Container Manager Client port

Description

The port number of the Ozone SCM block client service.

Related Name

ozone.scm.client.port

Default Value

9860

API Name

ozone.scm.client.port

Required

false

Storage Container Manager Datanode port

Description

The port number of the Ozone SCM service.

Related Name

ozone.scm.datanode.port

Default Value

9861

API Name

ozone.scm.datanode.port

Required

false

Storage Container Manager GRPC port

Description

Port used by SCM for Grpc Server.

Related Name

ozone.scm.grpc.port

Default Value

9895

API Name

ozone.scm.grpc.port

Required

false

Storage Container Manager HTTP Web UI Port

Description

The base port that the Storage Container Manager web user interface listens on. The host name of the Storage Container Manager is combined with this port to form the 'ozone.scm.http-address'.

Related Name

ozone.scm.http-port

Default Value

9876

API Name

ozone.scm.http-port

Required

true

Secure Storage Container Manager Web UI Port (TLS/SSL)

Description

The base port that the Storage Container Manager web user interface listens on when using HTTPS. The host name of the Storage Container Manager is combined with this port to form the 'ozone.scm.https-address'.

Related Name

ozone.scm.https-port

Default Value

9877

API Name

ozone.scm.https-port

Required

false

Storage Container Manager Ratis port

Description

The base port that SCM's Ratis Server listens on if multiple SCM's are configured.

Related Name

ozone.scm.ratis.port

Default Value

9894

API Name

ozone.scm.ratis.port

Required

false

Storage Container Manager Security Service port

Description

SCM security server port.

Related Name

ozone.scm.security.service.port

Default Value

9961

API Name

ozone.scm.security.service.port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Storage Container Manager roles.

Related Name

Default Value

scm

API Name

kerberos_role_princ_name

Required

true

Storage Container Manager TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Storage Container Manager might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Storage Container Manager TLS/SSL Trust Store Password

Description

The password for the Storage Container Manager TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Storage Container Manager

Description

Encrypt communication between clients and Storage Container Manager using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ozone.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Storage Container Manager TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Storage Container Manager is acting as a TLS/SSL server.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Storage Container Manager TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Storage Container Manager is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Storage Container Manager TLS/SSL Server Keystore File Password

Description

The password for the Storage Container Manager keystore file.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Balancing Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Balancing Interval parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.balancing.iteration.interval

Required

true

Suppress Parameter Validation: Exclude Containers from Balancing

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Containers from Balancing parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.exclude.containers

Required

true

Suppress Parameter Validation: Exclude Datanodes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Datanodes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.exclude.datanodes

Required

true

Suppress Parameter Validation: Include Datanodes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Include Datanodes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.include.datanodes

Required

true

Suppress Parameter Validation: Container Move Replication Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Move Replication Timeout parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.move.replication.timeout

Required

true

Suppress Parameter Validation: Container Move Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Move Timeout parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.move.timeout

Required

true

Suppress Parameter Validation: Maximum Size Entering Target

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Maximum Size Entering Target parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.entering.target.max

Required

true

Suppress Parameter Validation: Maximum Size Leaving Source

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Maximum Size Leaving Source parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.leaving.source.max

Required

true

Suppress Parameter Validation: Maximum Size to Move in Balancing

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Maximum Size to Move in Balancing parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.container.balancer.size.moved.max.per.iteration

Required

true

Suppress Parameter Validation: Over Replication Processing Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Over Replication Processing Interval parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.over.replicated.interval

Required

true

Suppress Parameter Validation: Replication Thread Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replication Thread Interval parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.thread.interval

Required

true

Suppress Parameter Validation: Under Replication Processing Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Under Replication Processing Interval parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.scm.replication.under.replicated.interval

Required

true

Suppress Parameter Validation: Datanode Container Protocol ACL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Datanode Container Protocol ACL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.security.client.datanode.container.protocol.acl

Required

true

Suppress Parameter Validation: SCM Client Certificate Protocol ACL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SCM Client Certificate Protocol ACL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hdds.security.client.scm.certificate.protocol.acl

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Storage Container Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Storage Container Manager Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Topology Script File Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Topology Script File Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_net.topology.script.file.name

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-policy.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/hadoop-policy.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/hadoop-policy.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ozone-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/scm-audit-log4j2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/scm-audit-log4j2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/scm-audit-log4j2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-client.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-client.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Advanced Configuration Snippet (Safety Valve) for ozone-conf/ssl-server.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone-conf/ssl-server.xml_role_safety_valve

Required

true

Suppress Parameter Validation: HSTS Header for Ozone SCM UI

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSTS Header for Ozone SCM UI parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.http.header.strict-transport-security

Required

true

Suppress Parameter Validation: Storage Container Manager Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Metadata Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.metadata.dirs

Required

true

Suppress Parameter Validation: Storage Container Manager Block Client port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Block Client port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.block.client.port

Required

true

Suppress Parameter Validation: Storage Container Manager Client port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Client port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.client.port

Required

true

Suppress Parameter Validation: Storage Container Manager Datanode port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Datanode port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.datanode.port

Required

true

Suppress Parameter Validation: Storage Container Manager Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.db.dirs

Required

true

Suppress Parameter Validation: Storage Container Manager GRPC port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager GRPC port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.grpc.port

Required

true

Suppress Parameter Validation: Storage Container Manager Ratis Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Ratis Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.ha.ratis.storage.dir

Required

true

Suppress Parameter Validation: Storage Container Manager HTTP Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager HTTP Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.http-bind-host

Required

true

Suppress Parameter Validation: Storage Container Manager HTTP Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager HTTP Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.http-port

Required

true

Suppress Parameter Validation: Secure Storage Container Manager HTTPS Bind Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Storage Container Manager HTTPS Bind Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.https-bind-host

Required

true

Suppress Parameter Validation: Secure Storage Container Manager Web UI Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Storage Container Manager Web UI Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.https-port

Required

true

Suppress Parameter Validation: Storage Container Manager Ratis port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Ratis port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.ratis.port

Required

true

Suppress Parameter Validation: Storage Container Manager Security Service port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Security Service port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ozone.scm.security.service.port

Required

true

Suppress Parameter Validation: Role Specific System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: Role Specific System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Specific System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_process_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Java Heap Size of Storage Container Manager

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of Storage Container Manager parameter.

Related Name

Default Value

false

API Name

role_config_suppression_scm_max_heap_size

Required

true

Suppress Parameter Validation: Storage Container Manager TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Storage Container Manager TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Storage Container Manager TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Storage Container Manager TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Storage Container Manager TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Storage Container Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Container Manager Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_storage_container_manager_role_env_safety_valve

Required

true

Suppress Health Test: Ozone SCM Safemode Canary

Description

Whether to suppress the results of the Ozone SCM Safemode Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_scm_safemode_canary

Required

true

Suppress Health Test: Ozone SCM Upgrade Need Finalization Canary

Description

Whether to suppress the results of the Ozone SCM Upgrade Need Finalization Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_scm_upgrade_need_finalization_canary

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ozone_storage_container_manager_unexpected_exits

Required

true

Phoenix Properties in Cloudera Runtime 7.2.18

Role groups:

Query Server

Advanced

Query Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Query Server Advanced Configuration Snippet (Safety Valve) for phoenix-site.xml

Description

For advanced use only. A string to be inserted into phoenix-site.xml for this role only.

Related Name

Default Value

API Name

phoenix-site.xml_role_safety_valve

Required

false

Query Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

PHOENIX_QUERY_SERVER_role_env_safety_valve

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from

publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Query Server Log Directory

Description

The log directory for log files of the role Query Server.

Related Name

log_dir

Default Value

/var/log/phoenix

API Name

log_dir

Required

false

Query Server Logging Threshold

Description

The minimum log level for Query Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Query Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Query Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Query Server Max Log Size

Description

The maximum size, in megabytes, per log file for Query Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.

- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

phoenix_query_server_fd_thresholds

Required

false

Query Server Host Health Test

Description

When computing the overall Query Server health, consider the host's health.

Related Name

Default Value

true

API Name

phoenix_query_server_host_health_enabled

Required

false

Query Server Process Health Test

Description

Enables the health test that the Query Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

phoenix_query_server_scm_health_enabled

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.

- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Remote User Extractor

Description

Boolean which controls if a remote user to impersonate should be extracted from the HTTP request parameter made by that user instead of the HTTP-authenticated user name (which is the default). Required for accessing Phoenix Query Server via Knox.

Related Name

phoenix.queryserver.withRemoteUserExtractor

Default Value

true

API Name

phoenix_query_server_with_remote_user_extractor

Required

false

Additional Phoenix Query Server Options

Description

These arguments are passed as part of the Java command line. Commonly, garbage collection flags or extra debugging flags are passed here.

Related Name

phoenix_queryserver_java_opts

Default Value

API Name

phoenix_queryserver_java_opts

Required

false

Phoenix Query Server Max Heapsize

Description

Maximum size for the Phoenix Query Server Java Process heap. Passed to Java -Xmx.

Related Name

phoenix_queryserver_max_heap_size

Default Value

2 GiB

API Name

phoenix_queryserver_max_heap_size

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Phoenix Query Server Port

Description

The port Phoenix Query Server will listen on

Related Name

phoenix.queryserver.http.port

Default Value

8765

API Name

phoenix_query_server_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Query Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Query Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

phoenix.queryserver.tls.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Query Server TLS/SSL Trust Store Password

Description

The password for the Query Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

phoenix.queryserver.tls.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Query Server

Description

Encrypt communication between clients and Query Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

phoenix.queryserver.tls.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Query Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Query Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

phoenix.queryserver.tls.keystore

Default Value

API Name

ssl_server_keystore_location

Required

false

Query Server TLS/SSL Server Keystore File Password

Description

The password for the Query Server keystore file.

Related Name

phoenix.queryserver.tls.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Query Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Query Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Query Server Advanced Configuration Snippet (Safety Valve) for phoenix-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server Advanced Configuration Snippet (Safety Valve) for phoenix-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Phoenix Query Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Phoenix Query Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_query_server_port

Required

true

Suppress Parameter Validation: Query Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_query_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Additional Phoenix Query Server Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Phoenix Query Server Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_queryserver_java_opts

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Query Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Query Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Query Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Query Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Query Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_phoenix_phoenix_query_server_unexpected_exits

Required

true

Service-Wide

Advanced

Phoenix Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

PHOENIX_service_env_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

phoenix

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

phoenix

API Name

process_username

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Query Server Monitoring Thresholds

Description

The health test thresholds of the overall Query Server health. The check returns "Concerning" health if the percentage of "Healthy" Query Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Query Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 90.0 %

API Name

PHOENIX_PHOENIX_QUERY_SERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HBase Service

Description

Name of the HBase service that this Phoenix service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

true

HDFS Service

Description

Name of the HDFS service that this Phoenix service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

ZooKeeper Service

Description

Name of the ZooKeeper service that this Phoenix service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

phoenix

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Query Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Query Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Query Server Log Directory

Description

Whether to suppress configuration warnings produced by the Query Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Query Server Advanced Configuration Snippet (Safety Valve) for phoenix-site.xml

Description

Whether to suppress configuration warnings produced by the Query Server Advanced Configuration Snippet (Safety Valve) for phoenix-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Phoenix Query Server Port

Description

Whether to suppress configuration warnings produced by the Phoenix Query Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_query_server_port

Required

true

Suppress Configuration Validator: Query Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Query Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_query_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Additional Phoenix Query Server Options

Description

Whether to suppress configuration warnings produced by the Additional Phoenix Query Server Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_phoenix_queryserver_java_opts

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Query Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Query Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Query Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Query Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Query Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Query Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Query Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Query Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: Phoenix HBase Dependency Write-Ahead Log (WAL) Codec Class Validator

Description

Whether to suppress configuration warnings produced by the Phoenix HBase Dependency Write-Ahead Log (WAL) Codec Class Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_phoenix_hbase_regionserver_wal_codec_validator

Required

true

Suppress Configuration Validator: Query Server Count Validator

Description

Whether to suppress configuration warnings produced by the Query Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_phoenix_query_server_count_validator

Required

true

Suppress Parameter Validation: Phoenix Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Phoenix Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_phoenix_service_env_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Query Server Health

Description

Whether to suppress the results of the Query Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_phoenix_phoenix_query_server_healthy

Required

true

Ranger Properties in Cloudera Runtime 7.2.18

Role groups:

Ranger Admin

Advanced

Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml

Description

For advanced use only. A string to be inserted into conf/ranger-admin-site.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-admin-site.xml_role_safety_valve

Required

false

Ranger Admin Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger Admin Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_ADMIN_role_env_safety_valve

Required

false

Logs

Ranger Admin Log Directory

Description

The log directory for log files of the role Ranger Admin.

Related Name

ranger.logs.base.dir

Default Value

/var/log/ranger/admin

API Name

log_dir

Required

false

Ranger Admin Logging Threshold

Description

The minimum log level for Ranger Admin logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger Admin Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger Admin logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger Admin Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger Admin logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_admin_fd_thresholds

Required

false

Ranger Admin Host Health Test

Description

When computing the overall Ranger Admin health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_admin_host_health_enabled

Required

false

Ranger Admin Process Health Test

Description

Enables the health test that the Ranger Admin's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_admin_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Ranger Admin Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

18 second(s)

API Name

graceful_stop_timeout

Required

false

Exclude Users from Audit Access Tab

Description

A single user, or a comma-separated list of multiple users that are excluded from Ranger audits when the Exclude Service Users checkbox is selected on the Ranger Audit Access tab in the Ranger Admin Web UI.

Related Name

ranger.accesslogs.exclude.users.list

Default Value

rangertagsync

API Name

ranger.accesslogs.exclude.users.list

Required

false

Kerberos Cookie Path

Description

Kerberos Cookie path

Related Name

ranger.admin.kerberos.cookie.path

Default Value

/

API Name

ranger.admin.kerberos.cookie.path

Required

false

Kerberos Token Valid Seconds

Description

Kerberos token validity

Related Name

ranger.admin.kerberos.token.valid.seconds

Default Value

30

API Name

ranger.admin.kerberos.token.valid.seconds

Required

false

Maximum Shards for Solr Collection of Ranger Audits

Description

Maximum number of shards for the Ranger Audit Solr collection. The recommended value is, number of replica given multiple by number of shards given for the collection.

Related Name

ranger.audit.solr.max.shards.per.node

Default Value

1

API Name

ranger.audit.solr.max.shards.per.node

Required

true

Replicas for Solr Collection of Ranger Audits

Description

Number of replicas for Ranger Audit Solr collection. The recommended value is, number of Solr servers running in the current cluster divided by number of shards for the collection.

Related Name

ranger.audit.solr.no.replica

Default Value

1

API Name

ranger.audit.solr.no.replica

Required

true

Shards for Solr Collection of Ranger Audits

Description

Number of shards required for Ranger Audit Solr collection. The recommended number of shards is equal or less than the number of Solr Server running in the current cluster.

Related Name

ranger.audit.solr.no.shards

Default Value

1

API Name

ranger.audit.solr.no.shards

Required

true

Enable Knox Trusted Proxy Support

Description

Determine if the Ranger service should allow authentication using Knox trusted proxy.

Related Name

ranger.authentication.allow.trustedproxy

Default Value

true

API Name

ranger.authentication.allow.trustedproxy

Required

false

Default Policy Groups

Description

Single or comma separated list of groups that are required in default policies for Ranger plugin services. The groups will be added for any new Ranger Plugin services created in Ranger Admin after setting value to this parameter.

Related Name

ranger.default.policy.groups

Default Value

API Name

ranger.default.policy.groups

Required

false

Default Policy Users

Description

Single or comma separated list of users that are required in default policies for Ranger plugin services. The users will be added for any new Ranger Plugin services created in Ranger Admin after setting value to this parameter.

Related Name

ranger.default.policy.users

Default Value

API Name

ranger.default.policy.users

Required

false

Admin AD Auth Base DN

Description

This parameter is only used if Authentication method is AD. The Distinguished Name (DN) of the starting point for directory server searches.

Related Name

ranger.ldap.ad.base.dn

Default Value

API Name

ranger.ldap.ad.base.dn

Required

false

Admin AD Auth Bind DN

Description

Full distinguished name (DN), including common name (CN), of an AD user account that has privileges to search for users. Only used if Authentication method is AD

Related Name

ranger.ldap.ad.bind.dn

Default Value

API Name

ranger.ldap.ad.bind.dn

Required

false

Admin AD Auth Domain Name

Description

AD domain. Only used if Authentication method is AD.

Related Name

ranger.ldap.ad.domain

Default Value

API Name

ranger.ldap.ad.domain

Required

false

Admin AD Auth Referral

Description

This parameter is only used if Authentication method is AD. Set to follow if multiple AD servers are configured to return continuation references for results. Set to ignore (default) if no referrals should be followed.

Related Name

ranger.ldap.ad.referral

Default Value

ignore

API Name

ranger.ldap.ad.referral

Required

false

Admin AD Auth URL

Description

AD URL. Only used if Authentication method is AD

Related Name

ranger.ldap.ad.url

Default Value

API Name

ranger.ldap.ad.url

Required

false

Admin AD Auth User Search Filter

Description

AD user search filter. Only used if Authentication method is AD.

Related Name

ranger.ldap.ad.user.searchfilter

Default Value

API Name

ranger.ldap.ad.user.searchfilter

Required

false

Admin LDAP Auth Base DN

Description

The Distinguished Name (DN) of the starting point for directory server searches. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.base.dn

Default Value

API Name

ranger.ldap.base.dn

Required

false

Admin LDAP Auth Bind User

Description

Full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search for users. This user is used for searching the users. This could be read-only LDAP user. Example: cn=admin,dc=example,dc=com

Related Name

ranger.ldap.bind.dn

Default Value

API Name

ranger.ldap.bind.dn

Required

false

Admin LDAP Auth Group Role Attribute

Description

LDAP group role attribute. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.group.roleattribute

Default Value

API Name

ranger.ldap.group.roleattribute

Required

false

Admin LDAP Auth Group Search Base

Description

LDAP group searchbase. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.group.searchbase

Default Value

API Name

ranger.ldap.group.searchbase

Required

false

Admin LDAP Auth Group Search Filter

Description

LDAP group search filter. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.group.searchfilter

Default Value

API Name

ranger.ldap.group.searchfilter

Required

false

Admin LDAP Auth Referral

Description

This parameter is only used if Authentication method is LDAP. Set to follow if multiple LDAP servers are configured to return continuation references for results. Set to ignore (default) if no referrals should be followed. When this parameter is set to throw, all of the normal entries are returned in the enumeration first, before the ReferralException is thrown.

Related Name

ranger.ldap.referral

Default Value

ignore

API Name

ranger.ldap.referral

Required

false

Admin LDAP Auth URL

Description

LDAP server URL. Example: value = ldap://localhost:389 or ldaps://localhost:636

Related Name

ranger.ldap.url

Default Value

API Name

ranger.ldap.url

Required

false

Admin LDAP Auth User DN Pattern

Description

LDAP user DN. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.user.dnpattern

Default Value

API Name

ranger.ldap.user.dnpattern

Required

false

Admin LDAP Auth User Search Filter

Description

LDAP user search filter. Only used if Authentication method is LDAP.

Related Name

ranger.ldap.user.searchfilter

Default Value

API Name

ranger.ldap.user.searchfilter

Required

false

SSO Browser Useragent

Description

Comma seperated values of browser agent

Related Name

ranger.sso.browser.useragent

Default Value

Mozilla, chrome

API Name

ranger.sso.browser.useragent

Required

false

Enable Ranger SSO

Description

Determine if Ranger is Knox SSO enabled or not ?

Related Name

ranger.sso.enabled

Default Value

false

API Name

ranger.sso.enabled

Required

false

SSO Provider Url

Description

SSO provider url Example: https://KNOX_HOST:KNOX_PORT/gateway/KNOXSSO_TOPOLOGY_NAME/api/v1/websso

Related Name

ranger.sso.providerurl

Default Value

API Name

ranger.sso.providerurl

Required

false

SSO Public Key

Description

Public key for SSO cookie verification

Related Name

ranger.sso.publicKey

Default Value

API Name

ranger.sso.publicKey

Required

false

Enable Auto Create Tag Service

Description

Whether to create tag service in Ranger Admin.

Related Name

ranger.tagservice.auto.create

Default Value

true

API Name

ranger.tagservice.auto.create

Required

false

Enable Tag Service Auto Link

Description

Whether to link the Tag service set in "Tag Service Name" parameter to all available services in Ranger Admin.

Related Name

ranger.tagservice.auto.link

Default Value

true

API Name

ranger.tagservice.auto.link

Required

false

Tag Service Name

Description

Name of the tag service that will be created in Ranger Admin when "Enable Auto Create Tag Service" parameter is enabled.

Related Name

ranger.tagservice.auto.name

Default Value

cm_tag

API Name

ranger.tagservice.auto.name

Required

false

Admin UNIX Auth Remote Login

Description

Whether remote login is enabled. Only used if Authentication method is UNIX.

Related Name

ranger.unixauth.remote.login.enabled

Default Value

true

API Name

ranger.unixauth.remote.login.enabled

Required

false

Admin UNIX Auth Service Hostname

Description

Host where unix authentication service is running. Only used if Authentication method is UNIX. {{RANGER_USERSYNC_HOST}} is a placeholder value which will be replaced with the host where Ranger Usersync will be installed in the current cluster.

Related Name

ranger.unixauth.service.hostname

Default Value

RANGER_USERSYNC_HOST

API Name

ranger.unixauth.service.hostname

Required

false

Ranger Admin Canary Health Enabled

Description

Ranger Admin Canary is enabled/disabled

Related Name

ranger_admin_canary_health_enabled

Default Value

true

API Name

ranger_admin_canary_health_enabled

Required

false

Ranger Admin Canary Health Timeout

Description

Timeout for Ranger Admin Canary health check

Related Name

ranger_admin_canary_health_timeout

Default Value

30 second(s)

API Name

ranger_admin_canary_health_timeout

Required

false

Ranger Admin Conf Path

Description

Staging directory for Ranger Admin Configuration. This should generally not be changed.

Related Name

ranger_admin_conf_path

Default Value

/etc/ranger/admin

API Name

ranger_admin_conf_path

Required

true

Ranger Admin Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

ranger_admin_max_heap_size

Default Value

1 GiB

API Name

ranger_admin_max_heap_size

Required

true

Admin Authentication Method

Description

Authentication Method for login to Ranger Admin.

Related Name

ranger.authentication.method

Default Value

PAM

API Name

ranger_authentication_method

Required

false

Ranger Database Host

Description

Hostname of the database used by Ranger Admin. If the port is non-default for your database type, use host:port notation.

Related Name

ranger_database_host

Default Value

API Name

ranger_database_host

Required

true

Ranger Database Name

Description

Name of Ranger Admin database.

Related Name

ranger_database_name

Default Value

ranger

API Name

ranger_database_name

Required

true

Ranger Database User Password

Description

Password for Ranger Admin database.

Related Name

ranger.jpa.jdbc.password

Default Value

API Name

ranger_database_password

Required

true

Ranger Database Type

Description

Database type to be used.

Related Name

ranger_database_type

Default Value

PostgreSQL

API Name

ranger_database_type

Required

true

Ranger Database User

Description

User for Ranger Admin database.

Related Name

ranger.jpa.jdbc.user

Default Value

rangeradmin

API Name

ranger_database_user

Required

true

Admin AD Auth Bind Password

Description

Password for the account that can search for users. Only used if Authentication method is AD

Related Name

ranger.ldap.ad.bind.password

Default Value

API Name

ranger_ldap_ad_bind_password

Required

false

Admin LDAP Auth Bind User Password

Description

Password for the account that can search for users.

Related Name

ranger.ldap.bind.password

Default Value

API Name

ranger_ldap_bind_password

Required

false

Knox Proxy User Groups

Description

Accepts a list of group names. The Knox user can impersonate only the users that belong to the groups specified in the list. The wildcard value * may be used to allow impersonation of any user belonging to any group.

Related Name

ranger.proxyuser.knox.groups

Default Value

*

API Name

ranger_proxyuser_knox_groups

Required

false

Knox Proxy User Hosts

Description

Accepts a list of IP addresses, IP address ranges in CIDR format and/or host names. The Knox user can impersonate only the requests coming from hosts specified in the list. The wildcard value * may be used to allow impersonation from any host.

Related Name

ranger.proxyuser.knox.hosts

Default Value

*

API Name

ranger_proxyuser_knox_hosts

Required

false

Knox Proxy User Users

Description

Accepts a list of usernames. The Knox user can impersonate only the users specified in the list. The wildcard value * may be used to allow impersonation of any user.

Related Name

ranger.proxyuser.knox.users

Default Value

*

API Name

ranger_proxyuser_knox_users

Required

false

Ranger Tomcat Work Dir

Description

Tomcat work directory for Ranger Admin. This should generally not be changed.

Related Name

ranger_tomcat_work_dir

Default Value

/var/lib/ranger/admin

API Name

ranger_tomcat_work_dir

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Admin Unix Auth Service Port

Description

Port for unix authentication service. Only used if Authentication method is UNIX.

Related Name

ranger.unixauth.service.port

Default Value

5151

API Name

ranger.unixauth.service.port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger Admin TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Admin might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ranger.truststore.file

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger Admin TLS/SSL Trust Store Password

Description

The password for the Ranger Admin TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ranger.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger Admin

Description

Encrypt communication between clients and Ranger Admin using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ranger.service.https.attrib.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ranger Admin TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Admin is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ranger.https.attrib.keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger Admin TLS/SSL Server Keystore File Password

Description

The password for the Ranger Admin keystore file.

Related Name

ranger.service.https.attrib.keystore.pass

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-admin-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger Admin Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger Admin Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Exclude Users from Audit Access Tab

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Users from Audit Access Tab parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.accesslogs.exclude.users.list

Required

true

Suppress Parameter Validation: Kerberos Cookie Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Cookie Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.admin.kerberos.cookie.path

Required

true

Suppress Parameter Validation: Default Policy Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Policy Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.default.policy.groups

Required

true

Suppress Parameter Validation: Default Policy Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Policy Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.default.policy.users

Required

true

Suppress Parameter Validation: Admin AD Auth Base DN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth Base DN parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.base.dn

Required

true

Suppress Parameter Validation: Admin AD Auth Bind DN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth Bind DN parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.bind.dn

Required

true

Suppress Parameter Validation: Admin AD Auth Domain Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth Domain Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.domain

Required

true

Suppress Parameter Validation: Admin AD Auth URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.url

Required

true

Suppress Parameter Validation: Admin AD Auth User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.user.searchfilter

Required

true

Suppress Parameter Validation: Admin LDAP Auth Base DN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Base DN parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.base.dn

Required

true

Suppress Parameter Validation: Admin LDAP Auth Bind User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Bind User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.bind.dn

Required

true

Suppress Parameter Validation: Admin LDAP Auth Group Role Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Group Role Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.roleattribute

Required

true

Suppress Parameter Validation: Admin LDAP Auth Group Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Group Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.searchbase

Required

true

Suppress Parameter Validation: Admin LDAP Auth Group Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Group Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.searchfilter

Required

true

Suppress Parameter Validation: Admin LDAP Auth URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.url

Required

true

Suppress Parameter Validation: Admin LDAP Auth User DN Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth User DN Pattern parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.user.dnpattern

Required

true

Suppress Parameter Validation: Admin LDAP Auth User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.user.searchfilter

Required

true

Suppress Parameter Validation: SSO Browser Useragent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSO Browser Useragent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.browser.useragent

Required

true

Suppress Parameter Validation: SSO Provider Url

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSO Provider Url parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.providerurl

Required

true

Suppress Parameter Validation: SSO Public Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSO Public Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.publickey

Required

true

Suppress Parameter Validation: Tag Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tag Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagservice.auto.name

Required

true

Suppress Parameter Validation: Admin UNIX Auth Service Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin UNIX Auth Service Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.unixauth.service.hostname

Required

true

Suppress Parameter Validation: Admin Unix Auth Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Unix Auth Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.unixauth.service.port

Required

true

Suppress Parameter Validation: Ranger Admin Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_conf_path

Required

true

Suppress Parameter Validation: Ranger Admin Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_max_heap_size

Required

true

Suppress Parameter Validation: Ranger Admin Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_role_env_safety_valve

Required

true

Suppress Parameter Validation: Ranger Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Database Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_host

Required

true

Suppress Parameter Validation: Ranger Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_name

Required

true

Suppress Parameter Validation: Ranger Database User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Database User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_password

Required

true

Suppress Parameter Validation: Ranger Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Database User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_user

Required

true

Suppress Parameter Validation: Admin AD Auth Bind Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin AD Auth Bind Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ldap_ad_bind_password

Required

true

Suppress Parameter Validation: Admin LDAP Auth Bind User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin LDAP Auth Bind User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ldap_bind_password

Required

true

Suppress Parameter Validation: Knox Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_groups

Required

true

Suppress Parameter Validation: Knox Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_hosts

Required

true

Suppress Parameter Validation: Knox Proxy User Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy User Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_users

Required

true

Suppress Parameter Validation: Ranger Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tomcat Work Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tomcat_work_dir

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger Admin TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger Admin TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger Admin TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger Admin TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Ranger Admin URL Canary Check

Description

Whether to suppress the results of the Ranger Admin URL Canary Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_admin_canary

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_admin_unexpected_exits

Required

true

Ranger Tagsync

Advanced

Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

For advanced use only. A string to be inserted into conf/atlas-application.properties for this role only.

Related Name

Default Value

API Name

conf/atlas-application.properties_role_safety_valve

Required

false

Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-tagsync-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-tagsync-policymgr-ssl.xml_role_safety_valve

Required

false

Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-site.xml

Description

For advanced use only. A string to be inserted into conf/ranger-tagsync-site.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-tagsync-site.xml_role_safety_valve

Required

false

Ranger Tagsync Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger Tagsync Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_TAGSYNC_role_env_safety_valve

Required

false

Logs

Ranger Tagsync Log Directory

Description

The log directory for log files of the role Ranger Tagsync.

Related Name

ranger.tagsync.logdir

Default Value

/var/log/ranger/tagsync

API Name

log_dir

Required

false

Ranger Tagsync Logging Threshold

Description

The minimum log level for Ranger Tagsync logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger Tagsync Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger Tagsync logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger Tagsync Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger Tagsync logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_tagsync_fd_thresholds

Required

false

Ranger Tagsync Host Health Test

Description

When computing the overall Ranger Tagsync health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_tagsync_host_health_enabled

Required

false

Ranger Tagsync Process Health Test

Description

Enables the health test that the Ranger Tagsync's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_tagsync_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Atlas Source: Kafka Consumer Group

Description

Kafka consumer group.

Related Name

atlas.kafka.entities.group.id

Default Value

ranger_entities_consumer

API Name

atlas.kafka.entities.group.id

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

18 second(s)

API Name

graceful_stop_timeout

Required

false

Capture Cluster name

Description

Capture cluster name.

Related Name

ranger.tagsync.atlas.default.cluster.name

Default Value

API Name

ranger.tagsync.atlas.default.cluster.name

Required

false

Enable Ranger Tagsync Cookie Authentication

Description

Enable cookie-based authentication for requests going from Ranger Tagsync to Ranger Admin.

Related Name

ranger.tagsync.cookie.enabled

Default Value

true

API Name

ranger.tagsync.cookie.enabled

Required

false

Ranger Tagsync Username

Description

Ranger Tagsync username in Ranger Admin.

Related Name

ranger.tagsync.dest.ranger.username

Default Value

rangertagsync

API Name

ranger.tagsync.dest.ranger.username

Required

false

Enable File Tag Source

Description

Whether to sync tags from file.

Related Name

ranger.tagsync.source.file

Default Value

false

API Name

ranger.tagsync.source.file

Required

false

File Source: File Update Polling Interval

Description

Sync Interval for updating tags from file.

Related Name

ranger.tagsync.source.file.check.interval.millis

Default Value

1 minute(s)

API Name

ranger.tagsync.source.file.check.interval.millis

Required

false

File Source: Filename

Description

Filename containing tags.

Related Name

ranger.tagsync.source.file.filename

Default Value

API Name

ranger.tagsync.source.file.filename

Required

false

Ranger Tagsync Conf Path

Description

Staging directory for Ranger Tagsync Configuration. This should generally not be changed.

Related Name

ranger_tagsync_conf_path

Default Value

/etc/ranger/tagsync

API Name

ranger_tagsync_conf_path

Required

true

Ranger Tagsync Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

ranger_tagsync_max_heap_size

Default Value

1 GiB

API Name

ranger_tagsync_max_heap_size

Required

true

Enable Ranger Tagsync Metrics

Description

Controls whether the Ranger Tagsync metrics are enabled.

Related Name

ranger.tagsync.metrics.enabled

Default Value

true

API Name

ranger_tagsync_metrics_enabled

Required

false

Ranger Tagsync Metrics File Name

Description

File name for the metrics exposed by Ranger Tagsync. The file is updated at the frequency configured by Ranger Tagsync Metrics Frequency.

Related Name

ranger.tagsync.metrics.filename

Default Value

metrics.json

API Name

ranger_tagsync_metrics_filename

Required

false

Ranger Tagsync Metrics File Path

Description

The location at which the metrics exposed by Ranger Tagsync will be written.

Related Name

ranger.tagsync.metrics.filepath

Default Value

/var/log/ranger/metrics-tagsync

API Name

ranger_tagsync_metrics_filepath

Required

false

Ranger Tagsync Metrics Frequency

Description

The frequency at which the metrics are logged at Ranger Tagsync Metrics File Path.

Related Name

ranger.tagsync.metrics.frequencytimeinmillis

Default Value

1 minute(s)

API Name

ranger_tagsync_metrics_frequency

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger Tagsync TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Tagsync might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

xasecure.policymgr.clientssl.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger Tagsync TLS/SSL Trust Store Password

Description

The password for the Ranger Tagsync TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

xasecure.policymgr.clientssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger Tagsync

Description

Encrypt communication between clients and Ranger Tagsync using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

Default Value

false

API Name

ssl_enabled

Required

false

Ranger Tagsync TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Tagsync is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

xasecure.policymgr.clientssl.keystore

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger Tagsync TLS/SSL Server Keystore File Password

Description

The password for the Ranger Tagsync keystore file.

Related Name

xasecure.policymgr.clientssl.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Atlas Source: Kafka Consumer Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Atlas Source: Kafka Consumer Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_atlas.kafka.entities.group.id

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/atlas-application.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-tagsync-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-tagsync-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger Tagsync Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger Tagsync Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Capture Cluster name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Capture Cluster name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.atlas.default.cluster.name

Required

true

Suppress Parameter Validation: Ranger Tagsync Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.dest.ranger.username

Required

true

Suppress Parameter Validation: File Source: Filename

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the File Source: Filename parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.source.file.filename

Required

true

Suppress Parameter Validation: Ranger Tagsync Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_conf_path

Required

true

Suppress Parameter Validation: Ranger Tagsync Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_max_heap_size

Required

true

Suppress Parameter Validation: Ranger Tagsync Metrics File Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Metrics File Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_metrics_filename

Required

true

Suppress Parameter Validation: Ranger Tagsync Metrics File Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Metrics File Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_metrics_filepath

Required

true

Suppress Parameter Validation: Ranger Tagsync Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_role_env_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger Tagsync TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger Tagsync TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger Tagsync TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger Tagsync TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_tagsync_unexpected_exits

Required

true

Ranger Usersync

Advanced

Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml

Description

For advanced use only. A string to be inserted into conf/ranger-ugsync-site.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-ugsync-site.xml_role_safety_valve

Required

false

Ranger Usersync Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger Usersync Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_USERSYNC_role_env_safety_valve

Required

false

Logs

Ranger Usersync Log Directory

Description

The log directory for log files of the role Ranger Usersync.

Related Name

ranger.usersync.logdir

Default Value

/var/log/ranger/usersync

API Name

log_dir

Required

false

Ranger Usersync Logging Threshold

Description

The minimum log level for Ranger Usersync logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger Usersync Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger Usersync logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger Usersync Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger Usersync logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_usersync_fd_thresholds

Required

false

Ranger Usersync Host Health Test

Description

When computing the overall Ranger Usersync health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_usersync_host_health_enabled

Required

false

Ranger Usersync Process Health Test

Description

Enables the health test that the Ranger Usersync's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_usersync_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

18 second(s)

API Name

graceful_stop_timeout

Required

false

Enable Ranger Usersync Cookie Authentication

Description

Enable cookie-based authentication for requests going from Ranger Usersync to Ranger Admin.

Related Name

ranger.usersync.cookie.enabled

Default Value

true

API Name

ranger.usersync.cookie.enabled

Required

false

Enable User Sync

Description

Should users and groups be synchronized to Ranger Database? Required to setup Ranger policies.

Related Name

ranger.usersync.enabled

Default Value

true

API Name

ranger.usersync.enabled

Required

false

Usersync Filesource File Name

Description

Path to the file with the users and groups information. Only used when Usersync Sync Source is set to "org.apache.ranger.unixusersync.process.FileSourceUserGroupBuilder". Example: /tmp/usergroup.json or /tmp/usergroup.csv or /tmp/usergroup.txt

Related Name

ranger.usersync.filesource.file

Default Value

API Name

ranger.usersync.filesource.file

Required

false

Usersync Filesource Delimiter

Description

Delimiter used in file, if File based user sync is used

Related Name

ranger.usersync.filesource.text.delimiter

Default Value

,

API Name

ranger.usersync.filesource.text.delimiter

Required

false

Ranger Usersync Group Based Role Assignment Rules

Description

The parameter is used to assign roles to users and groups synced in Ranger Admin. Based on the given values specified in the above delimiter parameters, Ranger Usersync will parse the value specified in this parameter and sync users and groups along with roles given. Example - "ROLE_SYS_ADMIN:u:username1,username2&ROLE_KEY_ADMIN:g:groupname1".

Related Name

ranger.usersync.group.based.role.assignment.rules

Default Value

API Name

ranger.usersync.group.based.role.assignment.rules

Required

false

Usersync Group Member Attribute

Description

LDAP group member attribute name. Example: member

Related Name

ranger.usersync.group.memberattributename

Default Value

API Name

ranger.usersync.group.memberattributename

Required

false

Usersync Group Name Attribute

Description

LDAP group name attribute. Example: cn

Related Name

ranger.usersync.group.nameattribute

Default Value

API Name

ranger.usersync.group.nameattribute

Required

false

Usersync Group Object Class

Description

LDAP Group object class. Example: group

Related Name

ranger.usersync.group.objectclass

Default Value

API Name

ranger.usersync.group.objectclass

Required

false

Usersync Enable Group Search First

Description

Enable Group Search First.

Related Name

ranger.usersync.group.search.first.enabled

Default Value

false

API Name

ranger.usersync.group.search.first.enabled

Required

false

Usersync Group Search Base

Description

Search base for groups. Sample value would be ou=groups,dc=hadoop,dc=apache,dc=org.
The parameter overrides value specified in ranger.usersync.ldap.searchBase, ranger.usersync.ldap.user.searchbase. If a value is not specified, takes the value of ranger.usersync.ldap.searchBase. If ranger.usersync.ldap.searchBase is also not specified, takes the value of ranger.usersync.ldap.user.searchbase. Multiple Ous can be configured with ; (semicolon) separated eg: ou=groups,DC=example,DC=com;ou=group1,ou=group2

Related Name

ranger.usersync.group.searchbase

Default Value

API Name

ranger.usersync.group.searchbase

Required

false

Usersync Enable Group Sync

Description

Whether Usersync should use ldapsearch to find groups instead of relying on user entry attributes.

Related Name

ranger.usersync.group.searchenabled

Default Value

true

API Name

ranger.usersync.group.searchenabled

Required

false

Usersync Group Search Filter

Description

Optional additional filter constraining the groups selected for syncing. A sample value would be (dept=eng)

Related Name

ranger.usersync.group.searchfilter

Default Value

API Name

ranger.usersync.group.searchfilter

Required

false

Usersync Group Search Scope

Description

Search scope for the groups. Value "base" indicates that only the entry specified as the search base in ranger.usersync.group.searchbase should be considered. One "indicates" that only the immediate children of the entry specified as the search base in ranger.usersync.group.searchbase should be considered. "Sub" indicates that the entry specified as the search base in ranger.usersync.group.searchbase, and all of its subordinates to any depth, should be considered.

Related Name

ranger.usersync.group.searchscope

Default Value

sub

API Name

ranger.usersync.group.searchscope

Required

false

Usersync Group Usermap Sync

Description

Whether to sync all groups for a user.

Related Name

ranger.usersync.group.usermapsyncenabled

Default Value

true

API Name

ranger.usersync.group.usermapsyncenabled

Required

false

Usersync Bind User

Description

Full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search for users. This user is used for searching the users. This could be read-only LDAP user. Example: cn=admin,dc=example,dc=com

Related Name

ranger.usersync.ldap.binddn

Default Value

API Name

ranger.usersync.ldap.binddn

Required

false

Usersync Incremental Sync

Description

Enable Incremental Sync.

Related Name

ranger.usersync.ldap.deltasync

Default Value

true

API Name

ranger.usersync.ldap.deltasync

Required

false

Usersync Group Hierarchy Levels

Description

Levels of LDAP directory tree where the groups need to be searched.

Related Name

ranger.usersync.ldap.grouphierarchylevels

Default Value

0

API Name

ranger.usersync.ldap.grouphierarchylevels

Required

false

Usersync Groupname Case Conversion

Description

Used for converting syncing groups to the selected case conversion.

Related Name

ranger.usersync.ldap.groupname.caseconversion

Default Value

none

API Name

ranger.usersync.ldap.groupname.caseconversion

Required

false

Usersync Referral

Description

Set to follow if multiple LDAP/AD servers are configured to return continuation references for results. Set to ignore if no referrals should be followed. When this parameter is set to throw, all of the normal entries are returned in the enumeration first, before the ReferralException is thrown.

Related Name

ranger.usersync.ldap.referral

Default Value

ignore

API Name

ranger.usersync.ldap.referral

Required

false

Usersync Search Base

Description

Search base for users and groups. Sample value would be dc=hadoop,dc=apache,dc=org.Multiple Ous can be configured with ; (semicolon) separated.

Related Name

ranger.usersync.ldap.searchBase

Default Value

API Name

ranger.usersync.ldap.searchBase

Required

false

Usersync Enable STARTTLS

Description

Enable LDAP STARTTLS.

Related Name

ranger.usersync.ldap.starttls

Default Value

false

API Name

ranger.usersync.ldap.starttls

Required

false

Usersync LDAP/AD URL

Description

LDAP server URL. Example: value = ldap://localhost:389 or ldaps://localhost:636

Related Name

ranger.usersync.ldap.url

Default Value

API Name

ranger.usersync.ldap.url

Required

false

Usersync User Group Name Attribute

Description

LDAP user group name attribute. Generally it is the same as username attribute. Example: sAMAccountName in AD, uid or cn in OpenLDAP

Related Name

ranger.usersync.ldap.user.groupnameattribute

Default Value

API Name

ranger.usersync.ldap.user.groupnameattribute

Required

false

Usersync User Name Attribute

Description

LDAP user name attribute. Example: sAMAccountName in AD, uid or cn in OpenLDAP

Related Name

ranger.usersync.ldap.user.nameattribute

Default Value

API Name

ranger.usersync.ldap.user.nameattribute

Required

false

Usersync User Object Class

Description

LDAP User Object Class. Example: person or user

Related Name

ranger.usersync.ldap.user.objectclass

Default Value

API Name

ranger.usersync.ldap.user.objectclass

Required

false

Usersync User Search Base

Description

Search base for users. Sample value would be ou=users,dc=hadoop,dc=apache,dc=org. Overrides value specified in ranger.usersync.ldap.searchBase. Multiple Ous can be configured with ; (semicolon) separated eg: cn=users,dc=example,dc=com;ou=example1,ou=example2

Related Name

ranger.usersync.ldap.user.searchbase

Default Value

API Name

ranger.usersync.ldap.user.searchbase

Required

false

Usersync User Search Filter

Description

Optional additional filter constraining the users selected for syncing. A sample value would be (dept=eng). Customize the value to suit your deployment.

Related Name

ranger.usersync.ldap.user.searchfilter

Default Value

API Name

ranger.usersync.ldap.user.searchfilter

Required

false

Usersync User Search Scope

Description

Search scope for the users. Value "base" indicates that only the entry specified as the search base in ranger.usersync.ldap.user.searchbase should be considered. "One" indicates that only the immediate children of the entry specified as the search base in ranger.usersync.ldap.user.searchbase should be considered. "Sub" indicates that the entry specified as the search base in ranger.usersync.ldap.user.searchbase, and all of its subordinates to any depth, should be considered.

Related Name

ranger.usersync.ldap.user.searchscope

Default Value

sub

API Name

ranger.usersync.ldap.user.searchscope

Required

false

Usersync Username Case Conversion

Description

Used for converting syncing users to the selected case conversion.

Related Name

ranger.usersync.ldap.username.caseconversion

Default Value

none

API Name

ranger.usersync.ldap.username.caseconversion

Required

false

Enable Results to be Paged for User/Group Request

Description

Whether results can be paged for User/Group requests.

Related Name

ranger.usersync.pagedresultsenabled

Default Value

true

API Name

ranger.usersync.pagedresultsenabled

Required

false

User/Group Request Page size.

Description

Enter Page size for User/Group Request.

Related Name

ranger.usersync.pagedresultssize

Default Value

500

API Name

ranger.usersync.pagedresultssize

Required

false

Maximum Records Per API Call

Description

Maximum number of records to be returned per API call.

Related Name

ranger.usersync.policymanager.maxrecordsperapicall

Default Value

1000

API Name

ranger.usersync.policymanager.maxrecordsperapicall

Required

true

Ranger Usersync Policymgr Username

Description

Ranger Usersync username in Ranger Admin.

Related Name

ranger.usersync.policymgr.username

Default Value

rangerusersync

API Name

ranger.usersync.policymgr.username

Required

false

Ranger Usersync Unix Service Port

Description

Port for Unix authentication service.

Related Name

ranger.usersync.port

Default Value

5151

API Name

ranger.usersync.port

Required

true

Ranger Usersync Role Assignment List Delimiter

Description

The parameter is used to specify delimiter while syncing roles to users and groups in Ranger Admin. It is a delimiter for roles. Example - "ROLE_SYS_ADMIN:u:username1,username2&ROLE_KEY_ADMIN:g:groupname1", where ROLE_SYS_ADMIN and ROLE_KEY_ADMIN are roles in Ranger Admin separated by delimiter &. Note - All the delimiters parameters ranger.usersync.role.assignment.list.delimiter, ranger.usersync.users.groups.assignment.list.delimiter and ranger.usersync.username.groupname.assignment.list.delimiter should have different values. The delimiters should not contain characters that are allowed in username or groupname.

Related Name

ranger.usersync.role.assignment.list.delimiter

Default Value

&

API Name

ranger.usersync.role.assignment.list.delimiter

Required

false

Usersync Sleeptime interval

Description

Sleep time interval between user sync operations in milliseconds.

Related Name

ranger.usersync.sleeptimeinmillisbetweensynccycle

Default Value

1 minute(s)

API Name

ranger.usersync.sleeptimeinmillisbetweensynccycle

Required

false

Source for Syncing User and Groups

Description

For syncing from Ldap source, use "org.apache.ranger.ldapusersync.process.LdapUserGroupBuilder". For syncing from Unix source, use "org.apache.ranger.unixusersync.process.UnixUserGroupBuilder". For syncing from File source, use "org.apache.ranger.unixusersync.process.FileSourceUserGroupBuilder"

Related Name

ranger.usersync.source.impl.class

Default Value

org.apache.ranger.unixusersync.process.UnixUserGroupBuilder

API Name

ranger.usersync.source.impl.class

Required

true

Ranger Usersync Unix Backend

Description

The backend mechanism to read users and groups from a UNIX system. The value is applicable only on UNIX-based systems.

Related Name

ranger.usersync.unix.backend

Default Value

nss

API Name

ranger.usersync.unix.backend

Required

false

Usersync UNIX Minimum User ID

Description

Minimum User ID to start syncing. This should be set to avoid syncing of UNIX system-level users in the Ranger Admin.

Related Name

ranger.usersync.unix.minUserId

Default Value

500

API Name

ranger.usersync.unix.minUserId

Required

false

Usersync Enable User Search

Description

Enable User Search, when ranger.usersync.group.search.first.enabled is set to true.

Related Name

ranger.usersync.user.searchenabled

Default Value

false

API Name

ranger.usersync.user.searchenabled

Required

false

Ranger Usersync Username Groupname Assignment List Delimiter

Description

The parameter is used to specify a delimiter while syncing users and groups in Ranger Admin. Used as a delimiter to differentiate between two or more users and groups. Example - "ROLE_SYS_ADMIN:u:username1,username2", where username1 and username2 are separated by ,. Note - All the delimiters parameters ranger.usersync.role.assignment.list.delimiter, ranger.usersync.users.groups.assignment.list.delimiter and ranger.usersync.username.groupname.assignment.list.delimiter should have different values. The delimiters should not contain characters that are allowed in username or groupname.

Related Name

ranger.usersync.username.groupname.assignment.list.delimiter

Default Value

,

API Name

ranger.usersync.username.groupname.assignment.list.delimiter

Required

false

Ranger Usersync User Groups Assignment List Delimiter

Description

The parameter is used to specify delimiter while syncing users and groups along with specified roles in Ranger Admin. It is a delimiter to differentiate between users and groups from respective roles. Example - "ROLE_SYS_ADMIN:u:username1,username2&ROLE_SYS_ADMIN:g:groupname1,groupname2", where ROLE_SYS_ADMIN is a role. "u" is used to denote the list of users followed by actual usernames which are username1 and username2. While "g" is used to denote the list of groups followed by actual groupnames which are groupname1 and groupname2. Note - All the delimiters parameters ranger.usersync.role.assignment.list.delimiter, ranger.usersync.users.groups.assignment.list.delimiter and ranger.usersync.username.groupname.assignment.list.delimiter should have different values. The delimiters should not contain characters that are allowed in username or groupname.

Related Name

ranger.usersync.users.groups.assignment.list.delimiter

Default Value

:

API Name

ranger.usersync.users.groups.assignment.list.delimiter

Required

false

Ranger Usersync Conf Path

Description

Staging directory for Ranger Usersync Configuration. This should generally not be changed.

Related Name

ranger_usersync_conf_path

Default Value

/etc/ranger/usersync

API Name

ranger_usersync_conf_path

Required

true

Usersync Bind User Password

Description

Password for the LDAP bind user used for searching users.

Related Name

ranger.usersync.ldap.ldapbindpassword

Default Value

API Name

ranger_usersync_ldap_ldapbindpassword

Required

false

Ranger Usersync Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

ranger_usersync_max_heap_size

Default Value

1 GiB

API Name

ranger_usersync_max_heap_size

Required

true

Enable Ranger Usersync Metrics

Description

Controls whether the Ranger Usersync metrics are enabled.

Related Name

ranger.usersync.metrics.enabled

Default Value

true

API Name

ranger_usersync_metrics_enabled

Required

false

Ranger Usersync Metrics File Name

Description

File name for the metrics exposed by Ranger Usersync. The file is updated at the frequency configured by Ranger Usersync Metrics Frequency.

Related Name

ranger.usersync.metrics.filename

Default Value

metrics.json

API Name

ranger_usersync_metrics_filename

Required

false

Ranger Usersync Metrics File Path

Description

The location at which the metrics exposed by Ranger Usersync will be written.

Related Name

ranger.usersync.metrics.filepath

Default Value

/var/log/ranger/metrics-usersync

API Name

ranger_usersync_metrics_filepath

Required

false

Ranger Usersync Metrics Frequency

Description

The frequency at which the metrics are logged at Ranger Usersync Metrics File Path.

Related Name

ranger.usersync.metrics.frequencytimeinmillis

Default Value

1 minute(s)

API Name

ranger_usersync_metrics_frequency

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger Usersync TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Usersync might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ranger.usersync.truststore.file

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger Usersync TLS/SSL Trust Store Password

Description

The password for the Ranger Usersync TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ranger.usersync.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-ugsync-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger Usersync Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger Usersync Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Usersync Filesource File Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Filesource File Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.filesource.file

Required

true

Suppress Parameter Validation: Usersync Filesource Delimiter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Filesource Delimiter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.filesource.text.delimiter

Required

true

Suppress Parameter Validation: Ranger Usersync Group Based Role Assignment Rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Group Based Role Assignment Rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.based.role.assignment.rules

Required

true

Suppress Parameter Validation: Usersync Group Member Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Group Member Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.memberattributename

Required

true

Suppress Parameter Validation: Usersync Group Name Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Group Name Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.nameattribute

Required

true

Suppress Parameter Validation: Usersync Group Object Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Group Object Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.objectclass

Required

true

Suppress Parameter Validation: Usersync Group Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Group Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.searchbase

Required

true

Suppress Parameter Validation: Usersync Group Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Group Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.searchfilter

Required

true

Suppress Parameter Validation: Usersync Bind User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Bind User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.binddn

Required

true

Suppress Parameter Validation: Usersync Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.searchbase

Required

true

Suppress Parameter Validation: Usersync LDAP/AD URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync LDAP/AD URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.url

Required

true

Suppress Parameter Validation: Usersync User Group Name Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync User Group Name Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.groupnameattribute

Required

true

Suppress Parameter Validation: Usersync User Name Attribute

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync User Name Attribute parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.nameattribute

Required

true

Suppress Parameter Validation: Usersync User Object Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync User Object Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.objectclass

Required

true

Suppress Parameter Validation: Usersync User Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync User Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.searchbase

Required

true

Suppress Parameter Validation: Usersync User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.searchfilter

Required

true

Suppress Parameter Validation: Ranger Usersync Policymgr Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Policymgr Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.policymgr.username

Required

true

Suppress Parameter Validation: Ranger Usersync Unix Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Unix Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.port

Required

true

Suppress Parameter Validation: Ranger Usersync Role Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Role Assignment List Delimiter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.role.assignment.list.delimiter

Required

true

Suppress Parameter Validation: Ranger Usersync Username Groupname Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Username Groupname Assignment List Delimiter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.username.groupname.assignment.list.delimiter

Required

true

Suppress Parameter Validation: Ranger Usersync User Groups Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync User Groups Assignment List Delimiter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.users.groups.assignment.list.delimiter

Required

true

Suppress Parameter Validation: Ranger Usersync Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Conf Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_conf_path

Required

true

Suppress Parameter Validation: Usersync Bind User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Usersync Bind User Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_ldap_ldapbindpassword

Required

true

Suppress Parameter Validation: Ranger Usersync Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_max_heap_size

Required

true

Suppress Parameter Validation: Ranger Usersync Metrics File Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Metrics File Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_metrics_filename

Required

true

Suppress Parameter Validation: Ranger Usersync Metrics File Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Metrics File Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_metrics_filepath

Required

true

Suppress Parameter Validation: Ranger Usersync Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_role_env_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger Usersync TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger Usersync TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_ranger_usersync_unexpected_exits

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

ranger

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

ranger

API Name

process_username

Required

true

Ranger Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

RANGER_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ranger Admin Monitoring Thresholds

Description

The health test thresholds of the overall Ranger Admin health. The check returns "Concerning" health if the percentage of "Healthy" Ranger Admins falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger Admins falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

RANGER_RANGER_ADMIN_healthy_thresholds

Required

false

Ranger Tagsync Role Health Test

Description

When computing the overall RANGER health, consider Ranger Tagsync's health

Related Name

Default Value

true

API Name

RANGER_RANGER_TAGSYNC_health_enabled

Required

false

Ranger Usersync Role Health Test

Description

When computing the overall RANGER health, consider Ranger Usersync's health

Related Name

Default Value

true

API Name

RANGER_RANGER_USERSYNC_health_enabled

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HDFS Service

Description

Name of the HDFS service that this Ranger service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Ranger KMS Keyadmin User Initial Password

Description

Password for the Ranger administrator, whose login name is "keyadmin". The password should be minimum 8 characters long, with at least one alphabetic and one numeric character. The following characters are invalid: " ' \ ` ´. Note that this password is only used to setup Ranger in the cluster: any subsequent changes will not be effective. This password can be later changed from the Ranger Admin UI under the user profile page.

Related Name

keyadmin_user_password

Default Value

API Name

keyadmin_user_password

Required

true

Load Balancer Address

Description

Load Balancer Address used by clients to access Ranger Admin. Only required when Ranger Admin is running with High Availability. Example: http://load-balancer-host:load-balancer-port

Related Name

ranger.externalurl

Default Value

API Name

load_balancer_url

Required

false

Ranger Plugin DFS Audit Enabled

Description

Whether DFS audit is enabled.

Related Name

ranger_plugin_hdfs_audit_enabled

Default Value

true

API Name

ranger_plugin_hdfs_audit_enabled

Required

false

Ranger Plugin DFS Audit URL

Description

An absolute URL with no trailing slash should be entered, or leave the value empty. Allows setting up a centralized storage location for Ranger audits. This URL is used as the base for audit directories: all services plugging into Ranger will prepend this URL to their configured path used to store Ranger audits.

Related Name

ranger_plugin_hdfs_audit_url

Default Value

/ranger/audit

API Name

ranger_plugin_hdfs_audit_url

Required

false

Ranger Admin User Initial Password

Description

Password for the Ranger administrator, whose login name is "admin". The password should be minimum 8 characters long, with at least one alphabetic and one numeric character. The following characters are invalid: " ' \ ` ´. Note that this password is only used to setup Ranger in the cluster: any subsequent changes will not be effective. This password can be later changed from the Ranger Admin UI under the user profile page.

Related Name

rangeradmin_user_password

Default Value

API Name

rangeradmin_user_password

Required

true

Ranger Tagsync User Initial Password

Description

Password for the Ranger administrator, whose login name is "rangertagsync". The password should be minimum 8 characters long, with at least one alphabetic and one numeric character. The following characters are invalid: " ' \ ` ´. Note that this password is only used to setup Ranger in the cluster: any subsequent changes will not be effective. This password can be later changed from the Ranger Admin UI under the user profile page.

Related Name

rangertagsync_user_password

Default Value

API Name

rangertagsync_user_password

Required

true

Ranger Usersync User Initial Password

Description

Password for the Ranger administrator, whose login name is "rangerusersync". The password should be minimum 8 characters long, with at least one alphabetic and one numeric character. The following characters are invalid: " ' \ ` ´. Note that this password is only used to setup Ranger in the cluster: any subsequent changes will not be effective. This password can be later changed from the Ranger Admin UI under the user profile page.

Related Name

rangerusersync_user_password

Default Value

API Name

rangerusersync_user_password

Required

true

Solr Service

Description

Name of the Solr service that this Ranger service instance depends on

Related Name

Default Value

API Name

solr_service

Required

true

Ports and Addresses

Admin HTTP Port

Description

HTTP Port for Ranger Admin.

Related Name

ranger.service.http.port

Default Value

6080

API Name

ranger_service_http_port

Required

true

Admin HTTPS port

Description

HTTPS Port for Ranger Admin. Only used when SSL is enabled for Ranger Admin.

Related Name

ranger.service.https.port

Default Value

6182

API Name

ranger_service_https_port

Required

true

Suppressions

Suppress Configuration Validator: Atlas Source: Kafka Consumer Group

Description

Whether to suppress configuration warnings produced by the Atlas Source: Kafka Consumer Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_atlas.kafka.entities.group.id

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/atlas-application.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/atlas-application.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-admin-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-tagsync-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Advanced Configuration Snippet (Safety Valve) for conf/ranger-tagsync-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-tagsync-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-ugsync-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Ranger Admin Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Admin Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Ranger Admin Log Directory

Description

Whether to suppress configuration warnings produced by the Ranger Admin Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Exclude Users from Audit Access Tab

Description

Whether to suppress configuration warnings produced by the Exclude Users from Audit Access Tab configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.accesslogs.exclude.users.list

Required

true

Suppress Configuration Validator: Kerberos Cookie Path

Description

Whether to suppress configuration warnings produced by the Kerberos Cookie Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.admin.kerberos.cookie.path

Required

true

Suppress Configuration Validator: Default Policy Groups

Description

Whether to suppress configuration warnings produced by the Default Policy Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.default.policy.groups

Required

true

Suppress Configuration Validator: Default Policy Users

Description

Whether to suppress configuration warnings produced by the Default Policy Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.default.policy.users

Required

true

Suppress Configuration Validator: Admin AD Auth Base DN

Description

Whether to suppress configuration warnings produced by the Admin AD Auth Base DN configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.base.dn

Required

true

Suppress Configuration Validator: Admin AD Auth Bind DN

Description

Whether to suppress configuration warnings produced by the Admin AD Auth Bind DN configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.bind.dn

Required

true

Suppress Configuration Validator: Admin AD Auth Domain Name

Description

Whether to suppress configuration warnings produced by the Admin AD Auth Domain Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.domain

Required

true

Suppress Configuration Validator: Admin AD Auth URL

Description

Whether to suppress configuration warnings produced by the Admin AD Auth URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.url

Required

true

Suppress Configuration Validator: Admin AD Auth User Search Filter

Description

Whether to suppress configuration warnings produced by the Admin AD Auth User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.ad.user.searchfilter

Required

true

Suppress Configuration Validator: Admin LDAP Auth Base DN

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Base DN configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.base.dn

Required

true

Suppress Configuration Validator: Admin LDAP Auth Bind User

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Bind User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.bind.dn

Required

true

Suppress Configuration Validator: Admin LDAP Auth Group Role Attribute

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Group Role Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.roleattribute

Required

true

Suppress Configuration Validator: Admin LDAP Auth Group Search Base

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Group Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.searchbase

Required

true

Suppress Configuration Validator: Admin LDAP Auth Group Search Filter

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Group Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.group.searchfilter

Required

true

Suppress Configuration Validator: Admin LDAP Auth URL

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.url

Required

true

Suppress Configuration Validator: Admin LDAP Auth User DN Pattern

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth User DN Pattern configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.user.dnpattern

Required

true

Suppress Configuration Validator: Admin LDAP Auth User Search Filter

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.ldap.user.searchfilter

Required

true

Suppress Configuration Validator: SSO Browser Useragent

Description

Whether to suppress configuration warnings produced by the SSO Browser Useragent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.browser.useragent

Required

true

Suppress Configuration Validator: SSO Provider Url

Description

Whether to suppress configuration warnings produced by the SSO Provider Url configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.providerurl

Required

true

Suppress Configuration Validator: SSO Public Key

Description

Whether to suppress configuration warnings produced by the SSO Public Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.sso.publickey

Required

true

Suppress Configuration Validator: Tag Service Name

Description

Whether to suppress configuration warnings produced by the Tag Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagservice.auto.name

Required

true

Suppress Configuration Validator: Capture Cluster name

Description

Whether to suppress configuration warnings produced by the Capture Cluster name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.atlas.default.cluster.name

Required

true

Suppress Configuration Validator: Ranger Tagsync Username

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.dest.ranger.username

Required

true

Suppress Configuration Validator: File Source: Filename

Description

Whether to suppress configuration warnings produced by the File Source: Filename configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.tagsync.source.file.filename

Required

true

Suppress Configuration Validator: Admin UNIX Auth Service Hostname

Description

Whether to suppress configuration warnings produced by the Admin UNIX Auth Service Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.unixauth.service.hostname

Required

true

Suppress Configuration Validator: Admin Unix Auth Service Port

Description

Whether to suppress configuration warnings produced by the Admin Unix Auth Service Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.unixauth.service.port

Required

true

Suppress Configuration Validator: Usersync Filesource File Name

Description

Whether to suppress configuration warnings produced by the Usersync Filesource File Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.filesource.file

Required

true

Suppress Configuration Validator: Usersync Filesource Delimiter

Description

Whether to suppress configuration warnings produced by the Usersync Filesource Delimiter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.filesource.text.delimiter

Required

true

Suppress Configuration Validator: Ranger Usersync Group Based Role Assignment Rules

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Group Based Role Assignment Rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.based.role.assignment.rules

Required

true

Suppress Configuration Validator: Usersync Group Member Attribute

Description

Whether to suppress configuration warnings produced by the Usersync Group Member Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.memberattributename

Required

true

Suppress Configuration Validator: Usersync Group Name Attribute

Description

Whether to suppress configuration warnings produced by the Usersync Group Name Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.nameattribute

Required

true

Suppress Configuration Validator: Usersync Group Object Class

Description

Whether to suppress configuration warnings produced by the Usersync Group Object Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.objectclass

Required

true

Suppress Configuration Validator: Usersync Group Search Base

Description

Whether to suppress configuration warnings produced by the Usersync Group Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.searchbase

Required

true

Suppress Configuration Validator: Usersync Group Search Filter

Description

Whether to suppress configuration warnings produced by the Usersync Group Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.group.searchfilter

Required

true

Suppress Configuration Validator: Usersync Bind User

Description

Whether to suppress configuration warnings produced by the Usersync Bind User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.binddn

Required

true

Suppress Configuration Validator: Usersync Search Base

Description

Whether to suppress configuration warnings produced by the Usersync Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.searchbase

Required

true

Suppress Configuration Validator: Usersync LDAP/AD URL

Description

Whether to suppress configuration warnings produced by the Usersync LDAP/AD URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.url

Required

true

Suppress Configuration Validator: Usersync User Group Name Attribute

Description

Whether to suppress configuration warnings produced by the Usersync User Group Name Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.groupnameattribute

Required

true

Suppress Configuration Validator: Usersync User Name Attribute

Description

Whether to suppress configuration warnings produced by the Usersync User Name Attribute configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.nameattribute

Required

true

Suppress Configuration Validator: Usersync User Object Class

Description

Whether to suppress configuration warnings produced by the Usersync User Object Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.objectclass

Required

true

Suppress Configuration Validator: Usersync User Search Base

Description

Whether to suppress configuration warnings produced by the Usersync User Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.searchbase

Required

true

Suppress Configuration Validator: Usersync User Search Filter

Description

Whether to suppress configuration warnings produced by the Usersync User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.ldap.user.searchfilter

Required

true

Suppress Configuration Validator: Ranger Usersync Policymgr Username

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Policymgr Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.policymgr.username

Required

true

Suppress Configuration Validator: Ranger Usersync Unix Service Port

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Unix Service Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.port

Required

true

Suppress Configuration Validator: Ranger Usersync Role Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Role Assignment List Delimiter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.role.assignment.list.delimiter

Required

true

Suppress Configuration Validator: Ranger Usersync Username Groupname Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Username Groupname Assignment List Delimiter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.username.groupname.assignment.list.delimiter

Required

true

Suppress Configuration Validator: Ranger Usersync User Groups Assignment List Delimiter

Description

Whether to suppress configuration warnings produced by the Ranger Usersync User Groups Assignment List Delimiter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.usersync.users.groups.assignment.list.delimiter

Required

true

Suppress Configuration Validator: Ranger Admin Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Admin Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_conf_path

Required

true

Suppress Configuration Validator: Ranger Admin Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger Admin Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_max_heap_size

Required

true

Suppress Configuration Validator: Ranger Admin Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Admin Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_admin_role_env_safety_valve

Required

true

Suppress Configuration Validator: Ranger Database Host

Description

Whether to suppress configuration warnings produced by the Ranger Database Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_host

Required

true

Suppress Configuration Validator: Ranger Database Name

Description

Whether to suppress configuration warnings produced by the Ranger Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_name

Required

true

Suppress Configuration Validator: Ranger Database User Password

Description

Whether to suppress configuration warnings produced by the Ranger Database User Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_password

Required

true

Suppress Configuration Validator: Ranger Database User

Description

Whether to suppress configuration warnings produced by the Ranger Database User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_database_user

Required

true

Suppress Configuration Validator: Admin AD Auth Bind Password

Description

Whether to suppress configuration warnings produced by the Admin AD Auth Bind Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ldap_ad_bind_password

Required

true

Suppress Configuration Validator: Admin LDAP Auth Bind User Password

Description

Whether to suppress configuration warnings produced by the Admin LDAP Auth Bind User Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_ldap_bind_password

Required

true

Suppress Configuration Validator: Knox Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_groups

Required

true

Suppress Configuration Validator: Knox Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_hosts

Required

true

Suppress Configuration Validator: Knox Proxy User Users

Description

Whether to suppress configuration warnings produced by the Knox Proxy User Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_proxyuser_knox_users

Required

true

Suppress Configuration Validator: Ranger Tagsync Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_conf_path

Required

true

Suppress Configuration Validator: Ranger Tagsync Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_max_heap_size

Required

true

Suppress Configuration Validator: Ranger Tagsync Metrics File Name

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Metrics File Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_metrics_filename

Required

true

Suppress Configuration Validator: Ranger Tagsync Metrics File Path

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Metrics File Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_metrics_filepath

Required

true

Suppress Configuration Validator: Ranger Tagsync Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tagsync_role_env_safety_valve

Required

true

Suppress Configuration Validator: Ranger Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the Ranger Tomcat Work Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_tomcat_work_dir

Required

true

Suppress Configuration Validator: Ranger Usersync Conf Path

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Conf Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_conf_path

Required

true

Suppress Configuration Validator: Usersync Bind User Password

Description

Whether to suppress configuration warnings produced by the Usersync Bind User Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_ldap_ldapbindpassword

Required

true

Suppress Configuration Validator: Ranger Usersync Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_max_heap_size

Required

true

Suppress Configuration Validator: Ranger Usersync Metrics File Name

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Metrics File Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_metrics_filename

Required

true

Suppress Configuration Validator: Ranger Usersync Metrics File Path

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Metrics File Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_metrics_filepath

Required

true

Suppress Configuration Validator: Ranger Usersync Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_usersync_role_env_safety_valve

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Ranger Admin TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Ranger Admin TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Ranger Admin TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Ranger Admin TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Ranger Admin TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Ranger Admin TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Ranger Admin TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Ranger Admin TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Ranger KMS Keyadmin User Initial Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Keyadmin User Initial Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_keyadmin_user_password

Required

true

Suppress Parameter Validation: Load Balancer Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Load Balancer Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_load_balancer_url

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Ranger Admin Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger Admin Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_admin_count_validator

Required

true

Suppress Parameter Validation: Ranger Plugin DFS Audit URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin DFS Audit URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_hdfs_audit_url

Required

true

Suppress Parameter Validation: Ranger Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_service_env_safety_valve

Required

true

Suppress Parameter Validation: Admin HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin HTTP Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_service_http_port

Required

true

Suppress Parameter Validation: Admin HTTPS port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin HTTPS port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_service_https_port

Required

true

Suppress Configuration Validator: Ranger Tagsync Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger Tagsync Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_tagsync_count_validator

Required

true

Suppress Configuration Validator: Ranger Usersync Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger Usersync Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_usersync_count_validator

Required

true

Suppress Parameter Validation: Ranger Admin User Initial Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Admin User Initial Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_rangeradmin_user_password

Required

true

Suppress Parameter Validation: Ranger Tagsync User Initial Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Tagsync User Initial Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_rangertagsync_user_password

Required

true

Suppress Parameter Validation: Ranger Usersync User Initial Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Usersync User Initial Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_rangerusersync_user_password

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Ranger Admin Health

Description

Whether to suppress the results of the Ranger Admin Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_ranger_admin_healthy

Required

true

Suppress Health Test: Ranger Tagsync Health

Description

Whether to suppress the results of the Ranger Tagsync Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_ranger_ranger_tagsync_health

Required

true

Suppress Health Test: Ranger Usersync Health

Description

Whether to suppress the results of the Ranger Usersync Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_ranger_ranger_usersync_health

Required

true

Ranger KMS Properties in Cloudera Runtime 7.2.18

Role groups:

Ranger KMS Server

Advanced

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

For advanced use only. A string to be inserted into conf/core-site.xml for this role only.

Related Name

Default Value

API Name

conf/core-site.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

For advanced use only. A string to be inserted into conf/dbks-site.xml for this role only.

Related Name

Default Value

API Name

conf/dbks-site.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

For advanced use only. A string to be inserted into conf/hdfs-site.xml for this role only.

Related Name

Default Value

API Name

conf/hdfs-site.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

For advanced use only. A string to be inserted into conf/kms-site.xml for this role only.

Related Name

Default Value

API Name

conf/kms-site.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-audit.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-audit.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-security.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-security.xml_role_safety_valve

Required

false

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-site.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-site.xml_role_safety_valve

Required

false

Ranger KMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger KMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_KMS_SERVER_role_env_safety_valve

Required

false

Logs

Ranger KMS Server Log Directory

Description

The log directory for log files of the role Ranger KMS Server.

Related Name

log_dir

Default Value

/var/log/ranger/kms

API Name

log_dir

Required

false

Ranger KMS Server Logging Threshold

Description

The minimum log level for Ranger KMS Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger KMS Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger KMS Server logs. Typically used by log4j or logback.

Related Name

Default Value
10

API Name
max_log_backup_index

Required
false

Ranger KMS Server Max Log Size

Description
The maximum size, in megabytes, per log file for Ranger KMS Server logs. Typically used by log4j or logback.

Related Name

Default Value
200 MiB

API Name
max_log_size

Required
false

Monitoring

Enable Health Alerts for this Role

Description
When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value
true

API Name
enable_alerts

Required
false

Enable Configuration Change Alerts

Description
When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value
false

API Name
enable_config_alerts

Required
false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_kms_server_fd_thresholds

Required

false

Ranger KMS Server Host Health Test

Description

When computing the overall Ranger KMS Server health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_kms_server_host_health_enabled

Required

false

Ranger KMS Server Process Health Test

Description

Enables the health test that the Ranger KMS Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_kms_server_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Ranger KMS Server Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

18 second(s)

API Name

graceful_stop_timeout

Required

false

Hadoop KMS Audit Aggregation Window In Milliseconds

Description

Duplicate audit log events within the aggregation window (specified in ms) are quashed to reduce log traffic. A single message for aggregated events is printed at the end of the window, along with a count of the number of aggregated events.

Related Name

hadoop.kms.audit.aggregation.window.ms

Default Value

10 second(s)

API Name

hadoop_kms_audit_aggregation_window_ms

Required

false

Hadoop KMS Authentication Signer Secret Provider

Description

Indicates how the secret to sign the authentication cookies will be stored. Options are 'random' (default), 'string' and 'zookeeper'. If using a setup with multiple KMS instances, 'zookeeper' should be used.

Related Name

hadoop.kms.authentication.signer.secret.provider

Default Value

random

API Name

hadoop_kms_authentication_signer_secret_provider

Required

false

Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type

Description

The Zookeeper authentication type, 'none' or kerberos.

Related Name

hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type

Default Value

none

API Name

hadoop_kms_authentication_signer_secret_provider_zookeeper_auth_type

Required

false

Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

The Zookeeper ZNode path where the KMS instances will store and retrieve the secret from.

Related Name

hadoop.kms.authentication.signer.secret.provider.zookeeper.path

Default Value

/hadoop-kms/hadoop-auth-signature-secret

API Name

hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

false

Hadoop KMS Blacklist Decrypt EEK

Description

Add user which is needed to be blacklist for decrypt EncryptedKey CryptoExtension operations. Multiple list os user's can be added with comma separated.

Related Name

hadoop.kms.blacklist.DECRYPT_EEK

Default Value

hdfs

API Name

hadoop_kms_blacklist_decrypt_eek

Required

false

Hadoop KMS Cache Enable

Description

Whether the KMS will act as a cache for the backing KeyProvider. When the cache is enabled, operations like getKeyVersion, getMetadata, and getCurrentKey will sometimes return cached data without consulting the backing KeyProvider. Cached values are flushed when keys are deleted or modified.

Related Name

hadoop.kms.cache.enable

Default Value

true

API Name

hadoop_kms_cache_enable

Required

false

Hadoop Kms Cache Timeout In Milliseconds

Description

Expiry time for the KMS key version and key metadata cache, in milliseconds. This affects getKeyVersion and getMetadata.

Related Name

hadoop.kms.cache.timeout.ms

Default Value

10 minute(s)

API Name

hadoop_kms_cache_timeout_ms

Required

false

Hadoop KMS Current Key Cache Timeout In Milliseconds

Description

Expiry time for the KMS current key cache, in milliseconds. This affects getCurrentKey operations.

Related Name

hadoop.kms.current.key.cache.timeout.ms

Default Value

30 second(s)

API Name

hadoop_kms_current_key_cache_timeout_ms

Required

false

HDFS Proxy User Groups

Description

Allows the hdfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hdfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_groups

Required

false

HDFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hdfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hdfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_hosts

Required

false

Hive Proxy User Groups

Description

Allows the hive superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hive.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hive_groups

Required

false

Hive Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hive user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hive.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hive_hosts

Required

false

HTTP Proxy User Groups

Description

Allows the HTTP superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.HTTP.groups

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_groups

Required

false

HTTP Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HTTP user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.HTTP.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_hosts

Required

false

HttpFS Proxy User Groups

Description

Allows the httpfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.httpfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_groups

Required

false

HttpFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the httpfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.httpfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_hosts

Required

false

Hue Proxy User Groups

Description

Allows the hue superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hue.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hue_groups

Required

false

Hue Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hue user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hue.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hue_hosts

Required

false

Livy Proxy User Groups

Description

Allows the livy superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.livy.groups

Default Value

*

API Name

hadoop_kms_proxyuser_livy_groups

Required

false

Livy Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the livy user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.livy.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_livy_hosts

Required

false

Mapred Proxy User Groups

Description

Allows the mapred superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.mapred.groups

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_groups

Required

false

Mapred Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the mapred user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.mapred.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_hosts

Required

false

Oozie Proxy User Groups

Description

Allows the oozie superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.oozie.groups

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_groups

Required

false

Oozie Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the oozie user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.oozie.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_hosts

Required

false

Ranger Proxy User Groups

Description

Allows the ranger superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.ranger.groups

Default Value

*

API Name

hadoop_kms_proxyuser_ranger_groups

Required

false

Ranger Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the ranger user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.ranger.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_ranger_hosts

Required

false

YARN Proxy User Groups

Description

Allows the yarn superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.yarn.groups

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_groups

Required

false

YARN Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the yarn user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.yarn.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_hosts

Required

false

Zeppelin Proxy User Groups

Description

Allows the zeppelin superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.zeppelin.groups

Default Value

*

API Name

hadoop_kms_proxyuser_zeppelin_groups

Required

false

Zeppelin Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the zeppelin user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.zeppelin.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_zeppelin_hosts

Required

false

Hadoop Security Keystore JavaKeyStoreProvider Password

Description

If using the JavaKeyStoreProvider, the password for the keystore file.

Related Name

hadoop.security.keystore.JavaKeyStoreProvider.password

Default Value

API Name

hadoop_security_keystore_javakeystoreprovider_password

Required

false

Azure Client ID

Description

Azure client id is a unique identifier generated by Azure AD that is tied to an application and service principal during its initial provisioning.

Related Name

ranger.kms.azure.client.id

Default Value

API Name

ranger_kms_azure_client_id

Required

false

Azure Client Secret

Description

Azure client secret to authenticate to key vault.

Related Name

ranger.kms.azure.client.secret

Default Value

API Name

ranger_kms_azure_client_secret

Required

false

Azure key vault cerificate password

Description

Azure key vault cerificate password.

Related Name

ranger.kms.azure.keyvault.certificate.password

Default Value

API Name

ranger_kms_azure_keyvault_certificate_password

Required

false

Azure Key Vault Cerificate Path

Description

Azure key vault cerificate path.

Related Name

ranger.kms.azure.keyvault.certificate.path

Default Value

API Name

ranger_kms_azure_keyvault_certificate_path

Required

false

Enable Azure Key Vault SSL

Description

Azure authentication via certificate or password.

Related Name

ranger.kms.azure.keyvault.ssl.enabled

Default Value

false

API Name

ranger_kms_azure_keyvault_ssl_enabled

Required

false

Azure Master Key Name

Description

Azure master key name.

Related Name

ranger.kms.azure.masterkey.name

Default Value

API Name

ranger_kms_azure_masterkey_name

Required

false

Azure Master Key Type

Description

Select the type for the Master key. Key Vault supports RSA and Elliptic Curve keys.

Related Name

ranger.kms.azure.masterkey.type

Default Value

RSA

API Name

ranger_kms_azure_masterkey_type

Required

false

Azure Zonekey Encryption Algorithm

Description

A supported algorithm for a encryption zone key operation.

Related Name

ranger.kms.azure.zonekey.encryption.algorithm

Default Value

RSA1_5

API Name

ranger_kms_azure_zonekey_encryption_algorithm

Required

false

Enable Azure Key Vault

Description

Whether to enable Azure key vault for secure key management.

Related Name

ranger.kms.azurekeyvault.enabled

Default Value

false

API Name

ranger_kms_azurekeyvault_enabled

Required

false

Azure Key Vault Url

Description

Azure Key Vault url of format "https://{keyvault-name}.vault.azure.net/", where keyvault-name is the name for a key vault in the Microsoft Azure Key Vault service.

Related Name

ranger.kms.azurekeyvault.url

Default Value

API Name

ranger_kms_azurekeyvault_url

Required

false

Enable Hardware Security Module (HSM) For Ranger KMS (Luna)

Description

Whether to enable HSM for protection of cryptographic keys.

Related Name

ranger.ks.hsm.enabled

Default Value

false

API Name

ranger_kms_hsm_enabled

Required

false

HSM Partition Name

Description

Independent logical HSM partition that resides within Luna SA appliance's physical K6 HSM appliances. It manage access controls, security policies and administration access. In case of high availabilty enter the group name.

Related Name

ranger.ks.hsm.partition.name

Default Value

API Name

ranger_kms_hsm_partition_name

Required

false

HSM partition password

Description

Password for securing HSM partition.

Related Name

ranger.ks.hsm.partition.password

Default Value

API Name

ranger_kms_hsm_partition_password

Required

false

HSM Type

Description

Select HSM type.

Related Name

ranger.ks.hsm.type

Default Value

LunaProvider

API Name

ranger_kms_hsm_type

Required

false

Enable SafeNet Keysecure For Ranger KMS

Description

Whether to enable Keysecure for secure and centralized key management.

Related Name

ranger.kms.keysecure.enabled

Default Value

false

API Name

ranger_kms_keysecure_enabled

Required

false

SafeNet Keysecure Hostname

Description

Hostname of SafeNet Keysecure.

Related Name

ranger.kms.keysecure.hostname

Default Value

API Name

ranger_kms_keysecure_hostname

Required

false

SafeNet Keysecure Login Password

Description

Login Password for accessing SafeNet Keysecure.

Related Name

ranger.kms.keysecure.login.password

Default Value

API Name

ranger_kms_keysecure_login_password

Required

false

SafeNet Keysecure Login Username

Description

Login Username for accessing SafeNet Keysecure.

Related Name

ranger.kms.keysecure.login.username

Default Value

API Name

ranger_kms_keysecure_login_username

Required

false

SafeNet Keysecure MasterKey Name

Description

Enter Keysecure masterkey Name. It is used for encrypting/decrypting zone keys.

Related Name

ranger.kms.keysecure.masterkey.name

Default Value

API Name

ranger_kms_keysecure_masterkey_name

Required

false

SafeNet Keysecure Masterkey Size

Description

SafeNet Keysecure Masterkey Size.

Related Name

ranger.kms.keysecure.masterkey.size

Default Value

256

API Name

ranger_kms_keysecure_masterkey_size

Required

false

SafeNet Keysecure Sunpkcs11 cfg Filepath

Description

SafeNet Keysecure sunpkcs11 cfg filepath.

Related Name

ranger.kms.keysecure.sunpkcs11.cfg.filepath

Default Value

API Name

ranger_kms_keysecure_sunpkcs11_cfg_filepath

Required

false

Enable SafeNet Keysecure User Password Authentication

Description

Whether to enable SafeNet Keysecure user password authentication.

Related Name

ranger.kms.keysecure.UserPassword.Authentication

Default Value

false

API Name

ranger_kms_keysecure_userpassword_authentication

Required

false

Ranger KMS Master Key Password

Description

Password for Ranger KMS Master Key.

Related Name

ranger.db.encrypt.key.password

Default Value

API Name

ranger_kms_master_key_password

Required

true

Ranger KMS Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

ranger_kms_max_heap_size

Default Value

1 GiB

API Name

ranger_kms_max_heap_size

Required

true

Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/kms/audit/hdfs/spool

API Name

ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Ranger KMS Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.kms.policy.cache.dir

Default Value

/var/lib/ranger/kms/policy-cache

API Name

ranger_kms_plugin_policy_cache_directory

Required

true

Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/kms/audit/solr/spool

API Name

ranger_kms_plugin_solr_audit_spool_directory

Required

true

Ranger Kms Server Canary Health Enabled

Description

Ranger Kms Server Canary is enabled/disabled

Related Name

ranger_kms_server_canary_health_enabled

Default Value

true

API Name

ranger_kms_server_canary_health_enabled

Required

false

Ranger Kms Server Canary Health Timeout

Description

Timeout for Ranger Kms Server Canary health check.

Related Name

ranger_kms_server_canary_health_timeout

Default Value

30 second(s)

API Name

ranger_kms_server_canary_health_timeout

Required

false

Ranger KMS Tomcat Work Dir

Description

Tomcat work directory for Ranger KMS. This should generally not be changed.

Related Name

ranger_kms_tomcat_work_dir

Default Value

/var/lib/ranger/kms

API Name

ranger_kms_tomcat_work_dir

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.kms.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.kms.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Ranger KMS HTTP Port

Description

HTTP Port for Ranger KMS.

Related Name

ranger.service.http.port

Default Value

9292

API Name

ranger_kms_http_port

Required

false

Ranger KMS HTTPS Port

Description

HTTPS Port for Ranger KMS. Only used when SSL is enabled for Ranger KMS.

Related Name

ranger.service.https.port

Default Value

9494

API Name

ranger_kms_https_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when

the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page

cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger KMS Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger KMS Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

xasecure.policymgr.clientssl.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger KMS Server TLS/SSL Trust Store Password

Description

The password for the Ranger KMS Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

xasecure.policymgr.clientssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger KMS Server

Description

Encrypt communication between clients and Ranger KMS Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ranger.service.https.attrib.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ranger KMS Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger KMS Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ranger.service.https.attrib.keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger KMS Server TLS/SSL Server Keystore File Password

Description

The password for the Ranger KMS Server keystore file.

Related Name

ranger.service.https.attrib.keystore.pass

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that

have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/core-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/dbks-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hdfs-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop KMS Authentication Signer Secret Provider Zookeeper Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

true

Suppress Parameter Validation: Hadoop KMS Blacklist Decrypt EEK

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop KMS Blacklist Decrypt EEK parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_blacklist_decrypt_eek

Required

true

Suppress Parameter Validation: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Parameter Validation: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Parameter Validation: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Parameter Validation: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Parameter Validation: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Parameter Validation: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Parameter Validation: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Parameter Validation: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_groups

Required

true

Suppress Parameter Validation: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_hosts

Required

true

Suppress Parameter Validation: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Parameter Validation: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Parameter Validation: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Parameter Validation: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Parameter Validation: Ranger Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_groups

Required

true

Suppress Parameter Validation: Ranger Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_hosts

Required

true

Suppress Parameter Validation: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Parameter Validation: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Parameter Validation: Zeppelin Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_groups

Required

true

Suppress Parameter Validation: Zeppelin Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_hosts

Required

true

Suppress Parameter Validation: Hadoop Security Keystore JavaKeyStoreProvider Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Security Keystore JavaKeyStoreProvider Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_keystore_javakeystoreprovider_password

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger KMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Azure Client ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure Client ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_client_id

Required

true

Suppress Parameter Validation: Azure Client Secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure Client Secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_client_secret

Required

true

Suppress Parameter Validation: Azure key vault cerificate password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure key vault cerificate password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_keyvault_certificate_password

Required

true

Suppress Parameter Validation: Azure Key Vault Cerificate Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure Key Vault Cerificate Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_keyvault_certificate_path

Required

true

Suppress Parameter Validation: Azure Master Key Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure Master Key Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_masterkey_name

Required

true

Suppress Parameter Validation: Azure Key Vault Url

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Azure Key Vault Url parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azurekeyvault_url

Required

true

Suppress Parameter Validation: HSM Partition Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSM Partition Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_hsm_partition_name

Required

true

Suppress Parameter Validation: HSM partition password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HSM partition password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_hsm_partition_password

Required

true

Suppress Parameter Validation: Ranger KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_http_port

Required

true

Suppress Parameter Validation: Ranger KMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_https_port

Required

true

Suppress Parameter Validation: SafeNet Keysecure Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SafeNet Keysecure Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_hostname

Required

true

Suppress Parameter Validation: SafeNet Keysecure Login Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SafeNet Keysecure Login Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_login_password

Required

true

Suppress Parameter Validation: SafeNet Keysecure Login Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SafeNet Keysecure Login Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_login_username

Required

true

Suppress Parameter Validation: SafeNet Keysecure MasterKey Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SafeNet Keysecure MasterKey Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_masterkey_name

Required

true

Suppress Parameter Validation: SafeNet Keysecure Sunpkcs11 cfg Filepath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SafeNet Keysecure Sunpkcs11 cfg Filepath parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_sunpkcs11_cfg_filepath

Required

true

Suppress Parameter Validation: Ranger KMS Master Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Master Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_master_key_password

Required

true

Suppress Parameter Validation: Ranger KMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_max_heap_size

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger KMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Tomcat Work Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_tomcat_work_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger KMS Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger KMS Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger KMS Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger KMS Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_ranger_kms_server_unexpected_exits

Required

true

Suppress Health Test: Ranger KMS URL Canary Check

Description

Whether to suppress the results of the Ranger KMS URL Canary Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_server_canary

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_username

Required

true

Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

RANGER_KMS_service_env_safety_valve

Required

false

Database

Ranger KMS Database Host

Description

Hostname of the database used by Ranger KMS. If the port is non-default for your database type, use host:port notation.

Related Name

ranger_kms_database_host

Default Value

localhost

API Name

ranger_kms_database_host

Required

true

Ranger KMS Database Name

Description

Name of Ranger KMS database.

Related Name

ranger_kms_database_name

Default Value

rangerkms

API Name

ranger_kms_database_name

Required

true

Ranger KMS Database User Password

Description

Password for Ranger KMS database.

Related Name

ranger.ks.jpa.jdbc.password

Default Value

API Name

ranger_kms_database_password

Required

true

Ranger KMS Database Port

Description

Port for Ranger KMS database.

Related Name

ranger_kms_database_port

Default Value

5432

API Name

ranger_kms_database_port

Required

true

Ranger KMS Database Type

Description

Database type to be used (postgres).

Related Name

ranger_kms_database_type

Default Value

postgresql

API Name

ranger_kms_database_type

Required

true

Ranger KMS Database User

Description

User for Ranger KMS database.

Related Name

ranger.ks.jpa.jdbc.user

Default Value

rangerkms

API Name

ranger_kms_database_user

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ranger KMS Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger KMS Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger KMS Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger KMS Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

RANGER_KMS_RANGER_KMS_SERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on

how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Ranger KMS Authentication Type

Description

Authentication type for the Ranger KMS. Can either be "simple" or "kerberos".

Related Name

hadoop.kms.authentication.type

Default Value

kerberos

API Name

hadoop_kms_authentication_type

Required

true

Ranger KMS Load Balancer

Description

Only required when Ranger KMS is running with High Availability.

Related Name

ranger_kms_load_balancer

Default Value

API Name

ranger_kms_load_balancer

Required

false

Ranger KMS Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_kms_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/kms

API Name

ranger_kms_plugin_hdfs_audit_directory

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Ranger KMS service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

rangerkms

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/core-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/dbks-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hdfs-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

Whether to suppress configuration warnings produced by the Hadoop KMS Authentication Signer Secret Provider Zookeeper Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

true

Suppress Configuration Validator: Hadoop KMS Blacklist Decrypt EEK

Description

Whether to suppress configuration warnings produced by the Hadoop KMS Blacklist Decrypt EEK configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_blacklist_decrypt_eek

Required

true

Suppress Configuration Validator: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Configuration Validator: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Configuration Validator: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Configuration Validator: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Configuration Validator: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Configuration Validator: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Configuration Validator: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Configuration Validator: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Configuration Validator: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Configuration Validator: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Configuration Validator: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_groups

Required

true

Suppress Configuration Validator: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_hosts

Required

true

Suppress Configuration Validator: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Configuration Validator: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Configuration Validator: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Configuration Validator: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Configuration Validator: Ranger Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Ranger Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_groups

Required

true

Suppress Configuration Validator: Ranger Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Ranger Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_hosts

Required

true

Suppress Configuration Validator: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Configuration Validator: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Configuration Validator: Zeppelin Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Zeppelin Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_groups

Required

true

Suppress Configuration Validator: Zeppelin Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Zeppelin Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_hosts

Required

true

Suppress Configuration Validator: Hadoop Security Keystore JavaKeyStoreProvider Password

Description

Whether to suppress configuration warnings produced by the Hadoop Security Keystore JavaKeyStoreProvider Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_keystore_javakeystoreprovider_password

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Ranger KMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server Log Directory

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Azure Client ID

Description

Whether to suppress configuration warnings produced by the Azure Client ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_client_id

Required

true

Suppress Configuration Validator: Azure Client Secret

Description

Whether to suppress configuration warnings produced by the Azure Client Secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_client_secret

Required

true

Suppress Configuration Validator: Azure key vault cerificate password

Description

Whether to suppress configuration warnings produced by the Azure key vault cerificate password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_keyvault_certificate_password

Required

true

Suppress Configuration Validator: Azure Key Vault Cerificate Path

Description

Whether to suppress configuration warnings produced by the Azure Key Vault Cerificate Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_keyvault_certificate_path

Required

true

Suppress Configuration Validator: Azure Master Key Name

Description

Whether to suppress configuration warnings produced by the Azure Master Key Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azure_masterkey_name

Required

true

Suppress Configuration Validator: Azure Key Vault Url

Description

Whether to suppress configuration warnings produced by the Azure Key Vault Url configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_azurekeyvault_url

Required

true

Suppress Configuration Validator: HSM Partition Name

Description

Whether to suppress configuration warnings produced by the HSM Partition Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_hsm_partition_name

Required

true

Suppress Configuration Validator: HSM partition password

Description

Whether to suppress configuration warnings produced by the HSM partition password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_hsm_partition_password

Required

true

Suppress Configuration Validator: Ranger KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the Ranger KMS HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_http_port

Required

true

Suppress Configuration Validator: Ranger KMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the Ranger KMS HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_https_port

Required

true

Suppress Configuration Validator: SafeNet Keysecure Hostname

Description

Whether to suppress configuration warnings produced by the SafeNet Keysecure Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_hostname

Required

true

Suppress Configuration Validator: SafeNet Keysecure Login Password

Description

Whether to suppress configuration warnings produced by the SafeNet Keysecure Login Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_login_password

Required

true

Suppress Configuration Validator: SafeNet Keysecure Login Username

Description

Whether to suppress configuration warnings produced by the SafeNet Keysecure Login Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_login_username

Required

true

Suppress Configuration Validator: SafeNet Keysecure MasterKey Name

Description

Whether to suppress configuration warnings produced by the SafeNet Keysecure MasterKey Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_masterkey_name

Required

true

Suppress Configuration Validator: SafeNet Keysecure Sunpkcs11 cfg Filepath

Description

Whether to suppress configuration warnings produced by the SafeNet Keysecure Sunpkcs11 cfg Filepath configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_keysecure_sunpkcs11_cfg_filepath

Required

true

Suppress Configuration Validator: Ranger KMS Master Key Password

Description

Whether to suppress configuration warnings produced by the Ranger KMS Master Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_master_key_password

Required

true

Suppress Configuration Validator: Ranger KMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger KMS Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_max_heap_size

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger KMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the Ranger KMS Tomcat Work Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_tomcat_work_dir

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Ranger KMS Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Ranger KMS Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Ranger KMS Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Ranger KMS Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger KMS Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Database Host parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_database_host

Required

true

Suppress Parameter Validation: Ranger KMS Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_database_name

Required

true

Suppress Parameter Validation: Ranger KMS Database User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Database User Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_database_password

Required

true

Suppress Parameter Validation: Ranger KMS Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_database_port

Required

true

Suppress Parameter Validation: Ranger KMS Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Database User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_database_user

Required

true

Suppress Parameter Validation: Ranger KMS Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Load Balancer parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_load_balancer

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_plugin_hdfs_audit_directory

Required

true

Suppress Configuration Validator: Ranger KMS Server Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_server_count_validator

Required

true

Suppress Parameter Validation: Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_service_env_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Ranger KMS Server Health

Description

Whether to suppress the results of the Ranger KMS Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_kms_ranger_kms_server_healthy

Required

true

Ranger KMS with Key Trustee Server Properties in Cloudera Runtime 7.2.18

Role groups:

Ranger KMS Server with KTS

Advanced

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

For advanced use only. A string to be inserted into conf/core-site.xml for this role only.

Related Name

Default Value

API Name

conf/core-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

For advanced use only. A string to be inserted into conf/dbks-site.xml for this role only.

Related Name

Default Value

API Name

conf/dbks-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

For advanced use only. A string to be inserted into conf/hdfs-site.xml for this role only.

Related Name

Default Value

API Name

conf/hdfs-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

For advanced use only. A string to be inserted into conf/kms-site.xml for this role only.

Related Name

Default Value

API Name

conf/kms-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kts-site.xml

Description

For advanced use only. A string to be inserted into conf/kts-site.xml for this role only.

Related Name

Default Value

API Name

conf/kts-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-audit.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-audit.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-security.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-security.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

For advanced use only. A string to be inserted into conf/ranger-kms-site.xml for this role only.

Related Name

Default Value

API Name

conf/ranger-kms-site.xml_role_safety_valve

Required

false

Ranger KMS Server with KTS Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from

publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger KMS Server with KTS Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_KMS_SERVER_KTS_role_env_safety_valve

Required

false

Logs

Ranger KMS Server with KTS Log Directory

Description

The log directory for log files of the role Ranger KMS Server with KTS.

Related Name

log_dir

Default Value

/var/log/ranger/kms

API Name

log_dir

Required

false

Ranger KMS Server with KTS Logging Threshold

Description

The minimum log level for Ranger KMS Server with KTS logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger KMS Server with KTS Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger KMS Server with KTS logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger KMS Server with KTS Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger KMS Server with KTS logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_kms_server_kts_fd_thresholds

Required

false

Ranger KMS Server with KTS Host Health Test

Description

When computing the overall Ranger KMS Server with KTS health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_kms_server_kts_host_health_enabled

Required

false

Ranger KMS Server with KTS Process Health Test

Description

Enables the health test that the Ranger KMS Server with KTS's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_kms_server_kts_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Key Trustee Server Auth Code

Description

Key Trustee Server auth code used for KMS to authenticate against the server

Related Name

cloudera.trustee.keyprovider.auth

Default Value

API Name

cloudera_trustee_keyprovider_auth

Required

true

Active Key Trustee Server

Description

Active Key Trustee Server hostname that backs the KMS.

Related Name

cloudera.trustee.keyprovider.hostname-ACTIVE

Default Value

API Name

cloudera_trustee_keyprovider_hostname-ACTIVE

Required

true

Passive Key Trustee Server

Description

Passive Key Trustee Server hostname that backs the KMS. Only needed for Key Trustee Server high availability.

Related Name

cloudera.trustee.keyprovider.hostname-PASSIVE

Default Value

API Name

cloudera_trustee_keyprovider_hostname-PASSIVE

Required

false

Key Trustee Server Org Name

Description

Key Trustee Server Organization that keys are stored against.

Related Name

cloudera.trustee.keyprovider.org

Default Value

API Name

cloudera_trustee_keyprovider_org

Required

true

Key Trustee Server Key Provider Pool Timeout

Description

Key Trustee key provider pool timeout.

Related Name

cloudera.trustee.keyprovider.pool.abandoned.timeout

Default Value

5 minute(s)

API Name

cloudera_trustee_keyprovider_pool_abandoned_timeout

Required

true

Key Trustee Server Key Provider Max Connections

Description

Key Trustee Server Key Provider Max Connections.

Related Name

cloudera.trustee.keyprovider.pool.max

Default Value

5

API Name

cloudera_trustee_keyprovider_pool_max

Required

true

Key Trustee Server Key Provider Pool Max Idle

Description

Key Trustee Server Key Provider Pool Max Idle.

Related Name

cloudera.trustee.keyprovider.pool.max.idle

Default Value

2

API Name

cloudera_trustee_keyprovider_pool_max_idle

Required

true

Key Trustee Server Key Provider Pool Min Idle

Description

Key Trustee Server Key Provider Pool Min Idle.

Related Name

cloudera.trustee.keyprovider.pool.min.idle

Default Value

1

API Name

cloudera_trustee_keyprovider_pool_min_idle

Required

true

Key Trustee Server Round Robin Reads

Description

Distribute read requests amongst the available Key Trustee Servers. Only effective when a passive server is specified.

Related Name

cloudera.trustee.keyprovider.roundrobin

Default Value

true

API Name

cloudera_trustee_keyprovider_roundrobin

Required

false

Ranger KMS Server with KTS Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

18 second(s)

API Name

graceful_stop_timeout

Required

false

Hadoop KMS Audit Aggregation Window

Description

Duplicate audit log events within the aggregation window (specified in ms) are quashed to reduce log traffic. A single message for aggregated events is printed at the end of the window, along with a count of the number of aggregated events.

Related Name

hadoop.kms.audit.aggregation.window.ms

Default Value

10 second(s)

API Name

hadoop_kms_audit_aggregation_window_ms

Required

false

Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type

Description

The Zookeeper authentication type, 'none' or kerberos.

Related Name

hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type

Default Value

none

API Name

hadoop_kms_authentication_signer_secret_provider_zookeeper_auth_type

Required

true

Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

The Zookeeper ZNode path where the KMS instances will store and retrieve the secret from.

Related Name

hadoop.kms.authentication.signer.secret.provider.zookeeper.path

Default Value

/hadoop-kms/hadoop-auth-signature-secret

API Name

hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

true

Hadoop KMS Blacklist Decrypt EEK

Description

Add user which is needed to be blacklist for decrypt EncryptedKey CryptoExtension operations. Multiple list os user's can be added with comma separated.

Related Name

hadoop.kms.blacklist.DECRYPT_EEK

Default Value

hdfs

API Name

hadoop_kms_blacklist_decrypt_eek

Required

false

Hadoop KMS Cache Enable

Description

Whether the KMS will act as a cache for the backing KeyProvider. When the cache is enabled, operations like getKeyVersion, getMetadata, and getCurrentKey will sometimes return cached data without consulting the backing KeyProvider. Cached values are flushed when keys are deleted or modified.

Related Name

hadoop.kms.cache.enable

Default Value

true

API Name

hadoop_kms_cache_enable

Required

false

Hadoop Kms Cache Timeout

Description

Expiry time for the KMS key version and key metadata cache, in milliseconds. This affects getKeyVersion and getMetadata.

Related Name

hadoop.kms.cache.timeout.ms

Default Value

10 minute(s)

API Name

hadoop_kms_cache_timeout_ms

Required

false

Hadoop KMS Current Key Cache Timeout

Description

Expiry time for the KMS current key cache, in milliseconds. This affects getCurrentKey operations.

Related Name

hadoop.kms.current.key.cache.timeout.ms

Default Value

30 second(s)

API Name

hadoop_kms_current_key_cache_timeout_ms

Required

false

HDFS Proxy User Groups

Description

Allows the hdfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hdfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_groups

Required

false

HDFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hdfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hdfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hdfs_hosts

Required

false

Hive Proxy User Groups

Description

Allows the hive superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hive.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hive_groups

Required

false

Hive Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hive user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hive.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hive_hosts

Required

false

HTTP Proxy User Groups

Description

Allows the HTTP superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.HTTP.groups

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_groups

Required

false

HTTP Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the HTTP user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.HTTP.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_HTTP_hosts

Required

false

HttpFS Proxy User Groups

Description

Allows the httpfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.httpfs.groups

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_groups

Required

false

HttpFS Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the httpfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.httpfs.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_httpfs_hosts

Required

false

Hue Proxy User Groups

Description

Allows the hue superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.hue.groups

Default Value

*

API Name

hadoop_kms_proxyuser_hue_groups

Required

false

Hue Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hue user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.hue.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_hue_hosts

Required

false

Livy Proxy User Groups

Description

Allows the livy superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.livy.groups

Default Value

*

API Name

hadoop_kms_proxyuser_livy_groups

Required

false

Livy Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the livy user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.livy.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_livy_hosts

Required

false

Mapred Proxy User Groups

Description

Allows the mapred superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.mapred.groups

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_groups

Required

false

Mapred Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the mapred user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.mapred.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_mapred_hosts

Required

false

Oozie Proxy User Groups

Description

Allows the oozie superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.oozie.groups

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_groups

Required

false

Oozie Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the oozie user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.oozie.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_oozie_hosts

Required

false

Ranger Proxy User Groups

Description

Allows the ranger superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.ranger.groups

Default Value

*

API Name

hadoop_kms_proxyuser_ranger_groups

Required

false

Ranger Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the ranger user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.ranger.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_ranger_hosts

Required

false

YARN Proxy User Groups

Description

Allows the yarn superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.yarn.groups

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_groups

Required

false

YARN Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the yarn user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.yarn.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_yarn_hosts

Required

false

Zeppelin Proxy User Groups

Description

Allows the zeppelin superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.kms.proxyuser.zeppelin.groups

Default Value

*

API Name

hadoop_kms_proxyuser_zeppelin_groups

Required

false

Zeppelin Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the zeppelin user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.kms.proxyuser.zeppelin.hosts

Default Value

*

API Name

hadoop_kms_proxyuser_zeppelin_hosts

Required

false

Key Trustee KeyStoreProvider Directory

Description

Directory to the keystore file used by Key Trustee KeyStoreProvider that backs the KMS.

Related Name

hadoop.kms.key.provider.uri

Default Value

/var/lib/kms-keytrustee

API Name

hadoop_security_key_provider_dir

Required

true

Hadoop Security Keystore JavaKeyStoreProvider Password

Description

If using the JavaKeyStoreProvider, the password for the keystore file.

Related Name

hadoop.security.keystore.JavaKeyStoreProvider.password

Default Value

API Name

hadoop_security_keystore_javakeystoreprovider_password

Required

false

Key Trustee KeyStoreProvider Configuration Directory

Description

Directory to store configuration of keystore file used by Key Trustee KeyStoreProvider that backs the KMS.

Related Name

keytrustee.kms.key.provider.conf.uri

Default Value

/var/lib/kms-keytrustee/keytrustee

API Name

keytrustee_security_key_provider_conf_dir

Required

true

Additional Java Configuration Options for KMS

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

kms_java_opts

Default Value

API Name

kms_java_opts

Required

false

Ranger KMS Max Heapsize

Description

Maximum size for the Java Process heap. Passed to Java -Xmx. Measured in megabytes.

Related Name

ranger_kms_max_heap_size

Default Value

1 GiB

API Name

ranger_kms_max_heap_size

Required

true

Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/kms/audit/hdfs/spool

API Name

ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Ranger KMS Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.kms.policy.cache.dir

Default Value

/var/lib/ranger/kms/policy-cache

API Name

ranger_kms_plugin_policy_cache_directory

Required

true

Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/kms/audit/solr/spool

API Name

ranger_kms_plugin_solr_audit_spool_directory

Required

true

Ranger Kms Kts Server Canary Health Enabled

Description

Ranger Kms Kts Server Canary is enabled/disabled

Related Name

ranger_kms_server_kts_canary_health_enabled

Default Value

true

API Name

ranger_kms_server_kts_canary_health_enabled

Required

false

Ranger Kms Kts Server Canary Health Timeout

Description

Timeout for Ranger Kms Kts Server Canary health check.

Related Name

ranger_kms_server_kts_canary_health_timeout

Default Value

30 second(s)

API Name

ranger_kms_server_kts_canary_health_timeout

Required

false

Ranger KMS Tomcat Work Dir

Description

Tomcat work directory for Ranger KMS. This should generally not be changed.

Related Name

ranger_kms_tomcat_work_dir

Default Value

/var/lib/ranger/kms

API Name

ranger_kms_tomcat_work_dir

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.kms.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.kms.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Ranger KMS HTTP Port

Description

HTTP Port for Ranger KMS.

Related Name

ranger.service.http.port

Default Value

9292

API Name

ranger_kms_http_port

Required

false

Ranger KMS HTTPS Port

Description

HTTPS Port for Ranger KMS. Only used when SSL is enabled for Ranger KMS.

Related Name

ranger.service.https.port

Default Value

9494

API Name

ranger_kms_https_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger KMS Server with KTS TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger KMS Server with KTS might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

xasecure.policymgr.clientssl.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger KMS Server with KTS TLS/SSL Trust Store Password

Description

The password for the Ranger KMS Server with KTS TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

xasecure.policymgr.clientssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger KMS Server with KTS

Description

Encrypt communication between clients and Ranger KMS Server with KTS using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ranger.service.https.attrib.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ranger KMS Server with KTS TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger KMS Server with KTS is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ranger.service.https.attrib.keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger KMS Server with KTS TLS/SSL Server Keystore File Password

Description

The password for the Ranger KMS Server with KTS keystore file.

Related Name

ranger.service.https.attrib.keystore.pass

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Key Trustee Server Auth Code

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Auth Code parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_auth

Required

true

Suppress Parameter Validation: Active Key Trustee Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Key Trustee Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_hostname-active

Required

true

Suppress Parameter Validation: Passive Key Trustee Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Passive Key Trustee Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_hostname-passive

Required

true

Suppress Parameter Validation: Key Trustee Server Org Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee Server Org Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_org

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/core-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/dbks-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hdfs-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kts-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kts-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kts-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop KMS Authentication Signer Secret Provider Zookeeper Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

true

Suppress Parameter Validation: Hadoop KMS Blacklist Decrypt EEK

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop KMS Blacklist Decrypt EEK parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_blacklist_decrypt_eek

Required

true

Suppress Parameter Validation: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Parameter Validation: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Parameter Validation: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Parameter Validation: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Parameter Validation: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Parameter Validation: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Parameter Validation: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HttpFS Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Parameter Validation: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_groups

Required

true

Suppress Parameter Validation: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_hosts

Required

true

Suppress Parameter Validation: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Parameter Validation: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Mapred Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Parameter Validation: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Parameter Validation: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Parameter Validation: Ranger Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_groups

Required

true

Suppress Parameter Validation: Ranger Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_hosts

Required

true

Suppress Parameter Validation: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Parameter Validation: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Parameter Validation: Zeppelin Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_groups

Required

true

Suppress Parameter Validation: Zeppelin Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_hosts

Required

true

Suppress Parameter Validation: Key Trustee KeyStoreProvider Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee KeyStoreProvider Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_key_provider_dir

Required

true

Suppress Parameter Validation: Hadoop Security Keystore JavaKeyStoreProvider Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Security Keystore JavaKeyStoreProvider Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_keystore_javakeystoreprovider_password

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Key Trustee KeyStoreProvider Configuration Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Key Trustee KeyStoreProvider Configuration Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_security_key_provider_conf_dir

Required

true

Suppress Parameter Validation: Additional Java Configuration Options for KMS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Additional Java Configuration Options for KMS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kms_java_opts

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ranger KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_http_port

Required

true

Suppress Parameter Validation: Ranger KMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_https_port

Required

true

Suppress Parameter Validation: Ranger KMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_max_heap_size

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_server_kts_role_env_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Tomcat Work Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_tomcat_work_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger KMS Server with KTS TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Server with KTS TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_kts_ranger_kms_server_kts_unexpected_exits

Required

true

Suppress Health Test: Ranger KMS KTS URL Canary Check

Description

Whether to suppress the results of the Ranger KMS KTS URL Canary Check heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_kms_server_kts_canary

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

kms

API Name

process_username

Required

true

Ranger KMS with Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

RANGER_KMS_KTS_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ranger KMS Server with KTS Monitoring Thresholds

Description

The health test thresholds of the overall Ranger KMS Server with KTS health. The check returns "Concerning" health if the percentage of "Healthy" Ranger KMS Server with KTSs falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger KMS Server with KTSs falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

RANGER_KMS_KTS_RANGER_KMS_SERVER_KTS_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Ranger KMS Authentication Type

Description

Authentication type for the Ranger KMS.

Related Name

hadoop.kms.authentication.type

Default Value

kerberos

API Name

hadoop_kms_authentication_type

Required

true

Ranger KMS Load Balancer

Description

Only required when Ranger KMS is running with High Availability.

Related Name

ranger_kms_load_balancer

Default Value

API Name

ranger_kms_load_balancer

Required

false

Ranger KMS Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_kms_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/kms

API Name

ranger_kms_plugin_hdfs_audit_directory

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Ranger KMS with Key Trustee Server service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

rangerkms

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Key Trustee Server Auth Code

Description

Whether to suppress configuration warnings produced by the Key Trustee Server Auth Code configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_auth

Required

true

Suppress Configuration Validator: Active Key Trustee Server

Description

Whether to suppress configuration warnings produced by the Active Key Trustee Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_hostname-active

Required

true

Suppress Configuration Validator: Passive Key Trustee Server

Description

Whether to suppress configuration warnings produced by the Passive Key Trustee Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_hostname-passive

Required

true

Suppress Configuration Validator: Key Trustee Server Org Name

Description

Whether to suppress configuration warnings produced by the Key Trustee Server Org Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_trustee_keyprovider_org

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/core-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/core-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/dbks-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/hdfs-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hdfs-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kts-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kts-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/kts-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/ranger-kms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/ranger-kms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Description

Whether to suppress configuration warnings produced by the Hadoop KMS Authentication Signer Secret Provider Zookeeper Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_authentication_signer_secret_provider_zookeeper_path

Required

true

Suppress Configuration Validator: Hadoop KMS Blacklist Decrypt EEK

Description

Whether to suppress configuration warnings produced by the Hadoop KMS Blacklist Decrypt EEK configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_blacklist_decrypt_eek

Required

true

Suppress Configuration Validator: HDFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_groups

Required

true

Suppress Configuration Validator: HDFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HDFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hdfs_hosts

Required

true

Suppress Configuration Validator: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_groups

Required

true

Suppress Configuration Validator: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hive_hosts

Required

true

Suppress Configuration Validator: HTTP Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_groups

Required

true

Suppress Configuration Validator: HTTP Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HTTP Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_http_hosts

Required

true

Suppress Configuration Validator: HttpFS Proxy User Groups

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_groups

Required

true

Suppress Configuration Validator: HttpFS Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the HttpFS Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_httpfs_hosts

Required

true

Suppress Configuration Validator: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_groups

Required

true

Suppress Configuration Validator: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_hue_hosts

Required

true

Suppress Configuration Validator: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_groups

Required

true

Suppress Configuration Validator: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_livy_hosts

Required

true

Suppress Configuration Validator: Mapred Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_groups

Required

true

Suppress Configuration Validator: Mapred Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Mapred Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_mapred_hosts

Required

true

Suppress Configuration Validator: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_groups

Required

true

Suppress Configuration Validator: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_oozie_hosts

Required

true

Suppress Configuration Validator: Ranger Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Ranger Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_groups

Required

true

Suppress Configuration Validator: Ranger Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Ranger Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_ranger_hosts

Required

true

Suppress Configuration Validator: YARN Proxy User Groups

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_groups

Required

true

Suppress Configuration Validator: YARN Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the YARN Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_yarn_hosts

Required

true

Suppress Configuration Validator: Zeppelin Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Zeppelin Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_groups

Required

true

Suppress Configuration Validator: Zeppelin Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Zeppelin Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_kms_proxyuser_zeppelin_hosts

Required

true

Suppress Configuration Validator: Key Trustee KeyStoreProvider Directory

Description

Whether to suppress configuration warnings produced by the Key Trustee KeyStoreProvider Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_key_provider_dir

Required

true

Suppress Configuration Validator: Hadoop Security Keystore JavaKeyStoreProvider Password

Description

Whether to suppress configuration warnings produced by the Hadoop Security Keystore JavaKeyStoreProvider Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_security_keystore_javakeystoreprovider_password

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Key Trustee KeyStoreProvider Configuration Directory

Description

Whether to suppress configuration warnings produced by the Key Trustee KeyStoreProvider Configuration Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_keytrustee_security_key_provider_conf_dir

Required

true

Suppress Configuration Validator: Additional Java Configuration Options for KMS

Description

Whether to suppress configuration warnings produced by the Additional Java Configuration Options for KMS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kms_java_opts

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Log Directory

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ranger KMS HTTP Port

Description

Whether to suppress configuration warnings produced by the Ranger KMS HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_http_port

Required

true

Suppress Configuration Validator: Ranger KMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the Ranger KMS HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_https_port

Required

true

Suppress Configuration Validator: Ranger KMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger KMS Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_max_heap_size

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger KMS Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger KMS Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_server_kts_role_env_safety_valve

Required

true

Suppress Configuration Validator: Ranger KMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the Ranger KMS Tomcat Work Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_kms_tomcat_work_dir

Required

true

Suppress Configuration Validator: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the Ranger Plugin Trusted Proxy IP Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger KMS with Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS with Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_kts_service_env_safety_valve

Required

true

Suppress Parameter Validation: Ranger KMS Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Load Balancer parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_load_balancer

Required

true

Suppress Parameter Validation: Ranger KMS Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger KMS Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_plugin_hdfs_audit_directory

Required

true

Suppress Configuration Validator: Ranger KMS Server with KTS Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger KMS Server with KTS Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_kms_server_kts_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Ranger KMS Server with KTS Health

Description

Whether to suppress the results of the Ranger KMS Server with KTS Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_kms_kts_ranger_kms_server_kts_healthy

Required

true

Ranger Raz Properties in Cloudera Runtime 7.2.18

Role groups:

Ranger Raz Server

Advanced

Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-audit.xml

Description

For advanced use only. A string to be inserted into ranger-raz-conf/ranger-raz-audit.xml for this role only.

Related Name

Default Value

API Name

ranger-raz-conf/ranger-raz-audit.xml_role_safety_valve

Required

false

Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-raz-conf/ranger-raz-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-raz-conf/ranger-raz-policymgr-ssl.xml_role_safety_valve

Required

false

Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-security.xml

Description

For advanced use only. A string to be inserted into ranger-raz-conf/ranger-raz-security.xml for this role only.

Related Name

Default Value

API Name

ranger-raz-conf/ranger-raz-security.xml_role_safety_valve

Required

false

Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-site.xml

Description

For advanced use only. A string to be inserted into ranger-raz-conf/ranger-raz-site.xml for this role only.

Related Name

Default Value

API Name

ranger-raz-conf/ranger-raz-site.xml_role_safety_valve

Required

false

Ranger Raz Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_RAZ_SERVER_role_env_safety_valve

Required

false

Logs

Ranger Raz Server Log Directory

Description

The log directory for log files of the role Ranger Raz Server.

Related Name

ranger.raz.log.dir

Default Value

/var/log/ranger/raz

API Name

log_dir

Required

false

Ranger Raz Server Logging Threshold

Description

The minimum log level for Ranger Raz Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger Raz Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger Raz Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger Raz Server Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger Raz Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_raz_server_fd_thresholds

Required

false

Ranger Raz Server Host Health Test

Description

When computing the overall Ranger Raz Server health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_raz_server_host_health_enabled

Required

false

Ranger Raz Server Process Health Test

Description

Enables the health test that the Ranger Raz Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_raz_server_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Raz Kerberos Cookie Path

Description

Raz Kerberos cookie path.

Related Name

ranger.raz.auth.method.dt.params.cookie.path

Default Value

/

API Name

ranger.raz.auth.method.dt.params.cookie.path

Required

false

Raz Kerberos Name Rules

Description

Raz Kerberos name rules.

Related Name

ranger.raz.auth.method.dt.params.kerberos.name.rules

Default Value

DEFAULT

API Name

ranger.raz.auth.method.dt.params.kerberos.name.rules

Required

false

Parameter Type for Kerberos Raz Authentication Method

Description

Indicates the parameter type used when kerberos Raz authentication method is enabled.

Related Name

ranger.raz.auth.method.dt.params.type

Default Value

kerberos

API Name

ranger.raz.auth.method.dt.params.type

Required

false

Raz Policy Cache Directory

Description

Directory where Raz policies are cached after successful retrieval from the source.

Related Name

ranger.raz.policy.cache.dir

Default Value

/var/lib/ranger/ranger-raz/policy-cache

API Name

ranger.raz.policy.cache.dir

Required

true

Raz Policy Poll Interval

Description

Time interval to poll for changes in Raz policies.

Related Name

ranger.raz.policy.pollIntervalMs

Default Value

30 second(s)

API Name

ranger.raz.policy.pollIntervalMs

Required

false

Connection Timeout for Raz Policy Rest Client

Description

Connection timeout for Raz policy rest client.

Related Name

ranger.raz.policy.rest.client.connection.timeoutMs

Default Value

2 minute(s)

API Name

ranger.raz.policy.rest.client.connection.timeoutMs

Required

false

Connection Timeout for Raz Policy Rest Read

Description

Connection timeout for Raz policy rest read.

Related Name

ranger.raz.policy.rest.read.timeoutMs

Default Value

2 minute(s)

API Name

ranger.raz.policy.rest.read.timeoutMs

Required

false

Raz Policy Rest Support Policy Deltas

Description

Raz Policy rest support policy deltas.

Related Name

ranger.raz.policy.rest.supports.policy.deltas

Default Value

false

API Name

ranger.raz.policy.rest.supports.policy.deltas

Required

false

Raz Policy Rest Support Tag Deltas

Description

Raz Policy rest support tag deltas.

Related Name

ranger.raz.tag.rest.supports.tag.deltas

Default Value

false

API Name

ranger.raz.tag.rest.supports.tag.deltas

Required

false

Raz Tomcat Ciphers

Description

A list of comma separated Tomcat ciphers supported by Raz server for SSL.

Related Name

ranger.raz.tomcat.ciphers

Default Value

API Name

ranger.raz.tomcat.ciphers

Required

false

Ranger Raz Azure Storage Accounts

Description

A comma-separated list of storage accounts from which user delegation keys will be created, cached, and renewed.

Related Name

ranger.raz.azure.storage.accounts

Default Value

API Name

ranger_raz_azure_storage_accounts

Required

false

Ranger Raz Max Heapsize

Description

Maximum size for the Java process heap. Passed to Java -Xmx.

Related Name

ranger_raz_max_heap_size

Default Value

1 GiB

API Name

ranger_raz_max_heap_size

Required

true

Ranger Raz Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/ranger-raz/audit/hdfs/spool

API Name

ranger_raz_plugin_hdfs_audit_spool_directory

Required

true

Ranger Raz Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.raz.policy.cache.dir

Default Value

/var/lib/ranger/ranger-raz/policy-cache

API Name

ranger_raz_plugin_policy_cache_directory

Required

true

Ranger Raz Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/ranger-raz/audit/solr/spool

API Name

ranger_raz_plugin_solr_audit_spool_directory

Required

true

Hive Proxy User Groups

Description

Allows the hive superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.hive.groups

Default Value

*

API Name

ranger_raz_proxyuser_hive_groups

Required

false

Hive Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hive user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.hive.hosts

Default Value

*

API Name

ranger_raz_proxyuser_hive_hosts

Required

false

Httpfs Proxy User Groups

Description

Allows the httpfs superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.httpfs.groups

Default Value

*

API Name

ranger_raz_proxyuser_httpfs_groups

Required

false

Httpfs Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the httpfs user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.httpfs.hosts

Default Value

*

API Name

ranger_raz_proxyuser_httpfs_hosts

Required

false

Hue Proxy User Groups

Description

Allows the hue superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.hue.groups

Default Value

*

API Name

ranger_raz_proxyuser_hue_groups

Required

false

Hue Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the hue user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.hue.hosts

Default Value

*

API Name

ranger_raz_proxyuser_hue_hosts

Required

false

Impala Proxy User Groups

Description

Allows the impala superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.impala.groups

Default Value

*

API Name

ranger_raz_proxyuser_impala_groups

Required

false

Impala Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the impala user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.impala.hosts

Default Value

*

API Name

ranger_raz_proxyuser_impala_hosts

Required

false

Livy Proxy User Groups

Description

Allows the livy superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.livy.groups

Default Value

*

API Name

ranger_raz_proxyuser_livy_groups

Required

false

Livy Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the livy user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.livy.hosts

Default Value

*

API Name

ranger_raz_proxyuser_livy_hosts

Required

false

Oozie Proxy User Groups

Description

Allows the oozie superuser to impersonate any members of a comma-delimited list of groups. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

ranger.raz.proxyuser.oozie.groups

Default Value

*

API Name

ranger_raz_proxyuser_oozie_groups

Required

false

Oozie Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the oozie user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

ranger.raz.proxyuser.oozie.hosts

Default Value

*

API Name

ranger_raz_proxyuser_oozie_hosts

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Raz HTTP Port

Description

The HTTP port for Ranger Raz.

Related Name

ranger.raz.service.http.port

Default Value

6081

API Name

ranger_raz_service_http_port

Required

false

Raz HTTPS Port

Description

The HTTPS port for Ranger Raz.

Related Name

ranger.raz.service.https.port

Default Value

6082

API Name

ranger_raz_service_https_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger Raz Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Raz Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

xasecure.policymgr.clientssl.truststore

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger Raz Server TLS/SSL Trust Store Password

Description

The password for the Ranger Raz Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

xasecure.policymgr.clientssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger Raz Server

Description

Encrypt communication between clients and Ranger Raz Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ranger.raz.service.https.attrib.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ranger Raz Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Raz Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ranger.raz.service.https.attrib.keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger Raz Server TLS/SSL Server Keystore File Password

Description

The password for the Ranger Raz Server keystore file.

Related Name

ranger.raz.service.https.attrib.keystore.pass

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger Raz Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Raz Kerberos Cookie Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz Kerberos Cookie Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.auth.method.dt.params.cookie.path

Required

true

Suppress Parameter Validation: Raz Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz Kerberos Name Rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.auth.method.dt.params.kerberos.name.rules

Required

true

Suppress Parameter Validation: Raz Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.policy.cache.dir

Required

true

Suppress Parameter Validation: Raz Tomcat Ciphers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz Tomcat Ciphers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.tomcat.ciphers

Required

true

Suppress Parameter Validation: Ranger Raz Azure Storage Accounts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Azure Storage Accounts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_azure_storage_accounts

Required

true

Suppress Parameter Validation: Ranger Raz Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_max_heap_size

Required

true

Suppress Parameter Validation: Ranger Raz Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Raz Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Raz Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hive_groups

Required

true

Suppress Parameter Validation: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hive_hosts

Required

true

Suppress Parameter Validation: Httpfs Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Httpfs Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_httpfs_groups

Required

true

Suppress Parameter Validation: Httpfs Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Httpfs Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_httpfs_hosts

Required

true

Suppress Parameter Validation: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hue_groups

Required

true

Suppress Parameter Validation: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hue Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hue_hosts

Required

true

Suppress Parameter Validation: Impala Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_impala_groups

Required

true

Suppress Parameter Validation: Impala Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Impala Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_impala_hosts

Required

true

Suppress Parameter Validation: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_livy_groups

Required

true

Suppress Parameter Validation: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Livy Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_livy_hosts

Required

true

Suppress Parameter Validation: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Groups parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_oozie_groups

Required

true

Suppress Parameter Validation: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oozie Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_oozie_hosts

Required

true

Suppress Parameter Validation: Ranger Raz Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Raz HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_service_http_port

Required

true

Suppress Parameter Validation: Raz HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Raz HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_service_https_port

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger Raz Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger Raz Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger Raz Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger Raz Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_raz_ranger_raz_server_unexpected_exits

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

ranger

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

rangerraz

API Name

process_username

Required

true

Ranger Raz Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

RANGER_RAZ_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ranger Raz Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger Raz Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger Raz Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger Raz Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

RANGER_RAZ_RANGER_RAZ_SERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

HDFS Service

Description

Name of the HDFS service that this Ranger Raz service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

Enable Kerberos Raz Authentication Method

Description

Indicates whether Kerberos is enabled.

Related Name

ranger.raz.auth.method.dt.params.kerberos

Default Value

true

API Name

ranger_raz_authentication_method_kerberos

Required

false

Ranger Raz Plugin Hdfs Audit Directory

Description

The DFS path on which Ranger audits are written.

Related Name

ranger_raz_plugin_hdfs_audit_directory

Default Value

$ranger_base_audit_url/rangerraz

API Name

ranger_raz_plugin_hdfs_audit_directory

Required

false

Ranger Service

Description

Name of the Ranger service that this Ranger Raz service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Ranger Raz service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

rangerraz

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Ranger Raz Server Log Directory

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-audit.xml

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-security.xml

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Advanced Configuration Snippet (Safety Valve) for ranger-raz-conf/ranger-raz-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-raz-conf/ranger-raz-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Raz Kerberos Cookie Path

Description

Whether to suppress configuration warnings produced by the Raz Kerberos Cookie Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.auth.method.dt.params.cookie.path

Required

true

Suppress Configuration Validator: Raz Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the Raz Kerberos Name Rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.auth.method.dt.params.kerberos.name.rules

Required

true

Suppress Configuration Validator: Raz Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the Raz Policy Cache Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.policy.cache.dir

Required

true

Suppress Configuration Validator: Raz Tomcat Ciphers

Description

Whether to suppress configuration warnings produced by the Raz Tomcat Ciphers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.raz.tomcat.ciphers

Required

true

Suppress Configuration Validator: Ranger Raz Azure Storage Accounts

Description

Whether to suppress configuration warnings produced by the Ranger Raz Azure Storage Accounts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_azure_storage_accounts

Required

true

Suppress Configuration Validator: Ranger Raz Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger Raz Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_max_heap_size

Required

true

Suppress Configuration Validator: Ranger Raz Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Raz Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Raz Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Raz Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_policy_cache_directory

Required

true

Suppress Configuration Validator: Ranger Raz Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Raz Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Hive Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hive_groups

Required

true

Suppress Configuration Validator: Hive Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hive Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hive_hosts

Required

true

Suppress Configuration Validator: Httpfs Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Httpfs Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_httpfs_groups

Required

true

Suppress Configuration Validator: Httpfs Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Httpfs Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_httpfs_hosts

Required

true

Suppress Configuration Validator: Hue Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hue_groups

Required

true

Suppress Configuration Validator: Hue Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Hue Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_hue_hosts

Required

true

Suppress Configuration Validator: Impala Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Impala Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_impala_groups

Required

true

Suppress Configuration Validator: Impala Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Impala Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_impala_hosts

Required

true

Suppress Configuration Validator: Livy Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_livy_groups

Required

true

Suppress Configuration Validator: Livy Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Livy Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_livy_hosts

Required

true

Suppress Configuration Validator: Oozie Proxy User Groups

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Groups configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_oozie_groups

Required

true

Suppress Configuration Validator: Oozie Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the Oozie Proxy User Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_proxyuser_oozie_hosts

Required

true

Suppress Configuration Validator: Ranger Raz Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Raz HTTP Port

Description

Whether to suppress configuration warnings produced by the Raz HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_service_http_port

Required

true

Suppress Configuration Validator: Raz HTTPS Port

Description

Whether to suppress configuration warnings produced by the Raz HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_raz_service_https_port

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Ranger Raz Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Ranger Raz Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Ranger Raz Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Ranger Raz Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Raz Plugin Hdfs Audit Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Plugin Hdfs Audit Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_raz_plugin_hdfs_audit_directory

Required

true

Suppress Configuration Validator: Ranger Raz Server Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger Raz Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_raz_server_count_validator

Required

true

Suppress Parameter Validation: Ranger Raz Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Raz Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_raz_service_env_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Ranger Raz Server Health

Description

Whether to suppress the results of the Ranger Raz Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_raz_ranger_raz_server_healthy

Required

true

Ranger RMS Properties in Cloudera Runtime 7.2.18

Role groups:

Ranger RMS Server

Advanced

Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for conf/hadoop-metrics2.properties

Description

For advanced use only. A string to be inserted into conf/hadoop-metrics2.properties for this role only.

Related Name

Default Value

API Name

conf/hadoop-metrics2.properties_role_safety_valve

Required

false

Ranger RMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j2.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-rms-conf/ranger-rms-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-rms-conf/ranger-rms-policymgr-ssl.xml_role_safety_valve

Required

false

Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-site.xml

Description

For advanced use only. A string to be inserted into ranger-rms-conf/ranger-rms-site.xml for this role only.

Related Name

Default Value

API Name

ranger-rms-conf/ranger-rms-site.xml_role_safety_valve

Required

false

Ranger RMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RANGER_RMS_SERVER_role_env_safety_valve

Required

false

Logs

Ranger RMS Server Log Directory

Description

The log directory for log files of the role Ranger RMS Server.

Related Name

ranger-rms.log.dir

Default Value

/var/log/ranger/rms

API Name

log_dir

Required

false

Ranger RMS Server Logging Threshold

Description

The minimum log level for Ranger RMS Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Ranger RMS Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Ranger RMS Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Ranger RMS Server Max Log Size

Description

The maximum size, in megabytes, per log file for Ranger RMS Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

ranger_rms_server_fd_thresholds

Required

false

Ranger RMS Server Host Health Test

Description

When computing the overall Ranger RMS Server health, consider the host's health.

Related Name

Default Value

true

API Name

ranger_rms_server_host_health_enabled

Required

false

Ranger RMS Server Process Health Test

Description

Enables the health test that the Ranger RMS Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

ranger_rms_server_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Ranger RMS JWKS Provider Url

Description

The {{JWKS_PROVIDER_URL}} is a placeholder value which will be replaced with the IDBroker endpoint to get JWKS (JSON Web Key Set) when present in the cluster. The placeholder can be replaced to have custom JWKS provider url endpoint.

Related Name

ranger-rms.auth.method.dt.params.jwks.provider-url

Default Value

JWKS_PROVIDER_URL

API Name

ranger-rms.auth.method.dt.params.jwks.provider-url

Required

false

Ranger RMS JWT Audiences

Description

List of comma separated audiences whose claims are supported by Ranger RMS service.

Related Name

ranger-rms.auth.method.dt.params.jwt.audiences

Default Value

idbroker, rms

API Name

ranger-rms.auth.method.dt.params.jwt.audiences

Required

false

Ranger RMS Server TLS/SSL Keystore File Alias

Description

The alias for the Ranger RMS Server TLS/SSL keystore file. User must configure the alias for the Ranger RMS keystore.

Related Name

ranger-rms.service.https.attrib.keystore.keyalias

Default Value

API Name

ranger-rms.service.https.attrib.keystore.keyalias

Required

false

Ranger RMS Access log Rotation Max Days

Description

The number of days to retain Ranger RMS Access logs before they are automatically rotated.

Related Name

ranger-rms.accesslog.rotate.max.days

Default Value

15

API Name

ranger-rms_accesslog_rotate_max_days

Required

false

Ranger RMS Client Java Opts

Description

These are Java command-line arguments for ranger rms. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

ranger_rms_client_java_opts

Default Value

API Name

ranger_rms_client_java_opts

Required

false

Enable Mapping Hive Managed Tables

Description

Ranger RMS, by default keeps track of external Hive table locations maintained in Hive Metastore. If Hive managed tables also need to be tracked, then enable this configuration.

Related Name

ranger-rms.HMS.map.managed.tables

Default Value

false

API Name

ranger_rms_hms_map_managed_tables

Required

false

Ranger RMS Hive Metastore Source Service Name

Description

Hdfs plugin service name managed in Ranger Admin. RMS needs to associate the HDFS locations with this service name before starting. Along with "Ranger RMS Hive Metastore Target Service Name" parameter, RMS will be able to map HMS data to RMS entities and persist them in RMS database. The default value points to default Hdfs plugin service name that gets created as a part of Ranger service installation from Cloudera Manager. Need to update the parameter value if using different Hdfs plugin service name in Ranger Admin.

Related Name

ranger-rms.HMS.source.service.name

Default Value

cm_hdfs

API Name

ranger_rms_hms_source_service_name

Required

false

Ranger RMS Hive Metastore Source Service Name for Ozone

Description

Ozone plugin service name managed in Ranger Admin. RMS needs to associate the OZONE locations with this service name before starting. Along with "Ranger RMS Hive Metastore Target Service Name" parameter, RMS will be able to map HMS data to Ozone entities and persist them in RMS database. The default value points to default Ozone plugin service name that gets created as a part of Ranger service installation from Cloudera Manager. Need to update the parameter value if using different Ozone plugin service name in Ranger Admin.

Related Name

ranger-rms.HMS.source.service.name.ozone

Default Value

cm_ozone

API Name

ranger_rms_hms_source_service_name_ozone

Required

false

Ranger RMS Hive Metastore Target Service Name

Description

Hive plugin service name managed in Ranger Admin. RMS need to associate the Hive tables with this service name before starting. The default value points to default Hive plugin service name that gets created as a part of Ranger service installation from Cloudera Manager. Need to update the parameter value if using different Hive plugin service name in Ranger Admin.

Related Name

ranger-rms.HMS.target.service.name

Default Value

cm_hive

API Name

ranger_rms_hms_target_service_name

Required

false

Ranger RMS Max Heapsize

Description

Maximum size for the Java process heap. Passed to Java -Xmx.

Related Name

ranger_rms_max_heap_size

Default Value

1 GiB

API Name

ranger_rms_max_heap_size

Required

true

Ranger RMS Polling Notifications Frequency

Description

Polling notifications frequency in milliseconds for Ranger RMS.

Related Name

ranger-rms.polling.notifications.frequency.ms

Default Value

30 second(s)

API Name

ranger_rms_polling_notifications_frequency_ms

Required

false

Ranger RMS Server HA

Description

Enable High availability for Ranger RMS server.

Related Name

ranger-rms.server.ha.enabled

Default Value

false

API Name

ranger_rms_server_ha_enabled

Required

false

Ranger RMS HA Zookeeper ACL

Description

Zookeeper ACL for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.acl

Default Value

auth:

API Name

ranger_rms_server_ha_zookeeper_acl

Required

false

Ranger RMS Server Zookeeper ACL Auth

Description

Zookeeper ACL Auth for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.auth

Default Value

API Name

ranger_rms_server_ha_zookeeper_acl_auth

Required

false

Ranger RMS Server HA Zookeeper Num Retries

Description

Number of retries to connect zookeeper for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.num.retries

Default Value

3

API Name

ranger_rms_server_ha_zookeeper_num_retries

Required

false

Ranger RMS Server HA Zookeeper Retry Sleeptime

Description

Zookeeper retry sleeptime in milliseconds for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.retry.sleeptime.ms

Default Value

1 second(s)

API Name

ranger_rms_server_ha_zookeeper_retry_sleeptime_ms

Required

false

Ranger RMS Server HA Zookeeper Session Timeout

Description

Zookeeper session timeout in milliseconds for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.session.timeout.ms

Default Value

20 second(s)

API Name

ranger_rms_server_ha_zookeeper_session_timeout_ms

Required

false

Ranger RMS Server HA Zookeeper Zkroot

Description

Zookeeper Zkroot for Ranger RMS server.

Related Name

ranger-rms.server.ha.zookeeper.zkroot

Default Value

/ranger-rms

API Name

ranger_rms_server_ha_zookeeper_zkroot

Required

false

Ranger RMS Server IDs

Description

Ranger RMS Server IDs.

Related Name

ranger-rms.server.ids

Default Value

API Name

ranger_rms_server_ids

Required

false

Ranger RMS Supported Uri Scheme

Description

Hive service storage type used to store Hive's tables.

Related Name

ranger-rms.supported.uri.scheme

Default Value

hdfs, o3fs, ofs

API Name

ranger_rms_supported_uri_scheme

Required

false

Ranger RMS Tomcat Work Dir

Description

Tomcat work directory for Ranger RMS.

Related Name

ranger-rms.tomcat.work.dir

Default Value

/var/lib/ranger/ranger-rms/work

API Name

ranger_rms_tomcat_work_dir

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

RMS HTTP Port

Description

The HTTP port for Ranger RMS.

Related Name

ranger-rms.service.http.port

Default Value

8383

API Name

ranger_rms_service_http_port

Required

false

RMS HTTPS Port

Description

The HTTPS port for Ranger RMS.

Related Name

ranger-rms.service.https.port

Default Value

8484

API Name

ranger_rms_service_https_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Ranger RMS Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger RMS Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ranger-rms.truststore.file

Default Value

API Name

ssl_client_truststore_location

Required

false

Ranger RMS Server TLS/SSL Trust Store Password

Description

The password for the Ranger RMS Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ranger-rms.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Ranger RMS Server

Description

Encrypt communication between clients and Ranger RMS Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ranger-rms.service.https.attrib.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Ranger RMS Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger RMS Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ranger-rms.service.https.attrib.keystore.file

Default Value

API Name

ssl_server_keystore_location

Required

false

Ranger RMS Server TLS/SSL Server Keystore File Password

Description

The password for the Ranger RMS Server keystore file.

Related Name

ranger-rms.service.https.attrib.keystore.pass

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user

with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for conf/hadoop-metrics2.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for conf/hadoop-metrics2.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hadoop-metrics2.properties_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Ranger RMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Ranger RMS Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms-conf/ranger-rms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms-conf/ranger-rms-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger RMS JWKS Provider Url

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS JWKS Provider Url parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.auth.method.dt.params.jwks.provider-url

Required

true

Suppress Parameter Validation: Ranger RMS JWT Audiences

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS JWT Audiences parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.auth.method.dt.params.jwt.audiences

Required

true

Suppress Parameter Validation: Ranger RMS Server TLS/SSL Keystore File Alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server TLS/SSL Keystore File Alias parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.service.https.attrib.keystore.keyalias

Required

true

Suppress Parameter Validation: Ranger RMS Client Java Opts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Client Java Opts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_client_java_opts

Required

true

Suppress Parameter Validation: Ranger RMS Hive Metastore Source Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Hive Metastore Source Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_source_service_name

Required

true

Suppress Parameter Validation: Ranger RMS Hive Metastore Source Service Name for Ozone

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Hive Metastore Source Service Name for Ozone parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_source_service_name_ozone

Required

true

Suppress Parameter Validation: Ranger RMS Hive Metastore Target Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Hive Metastore Target Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_target_service_name

Required

true

Suppress Parameter Validation: Ranger RMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Max Heapsize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_max_heap_size

Required

true

Suppress Parameter Validation: Ranger RMS HA Zookeeper ACL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS HA Zookeeper ACL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_acl

Required

true

Suppress Parameter Validation: Ranger RMS Server Zookeeper ACL Auth

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Zookeeper ACL Auth parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_acl_auth

Required

true

Suppress Parameter Validation: Ranger RMS Server HA Zookeeper Zkroot

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server HA Zookeeper Zkroot parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_zkroot

Required

true

Suppress Parameter Validation: Ranger RMS Server IDs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server IDs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ids

Required

true

Suppress Parameter Validation: Ranger RMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: RMS HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RMS HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_service_http_port

Required

true

Suppress Parameter Validation: RMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RMS HTTPS Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_service_https_port

Required

true

Suppress Parameter Validation: Ranger RMS Supported Uri Scheme

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Supported Uri Scheme parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_supported_uri_scheme

Required

true

Suppress Parameter Validation: Ranger RMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Tomcat Work Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_tomcat_work_dir

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Ranger RMS Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Ranger RMS Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Ranger RMS Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Ranger RMS Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_ranger_rms_ranger_rms_server_unexpected_exits

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

ranger

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

rangerrms

API Name

process_username

Required

true

Ranger RMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

RANGER_RMS_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Ranger RMS Server Monitoring Thresholds

Description

The health test thresholds of the overall Ranger RMS Server health. The check returns "Concerning" health if the percentage of "Healthy" Ranger RMS Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Ranger RMS Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 49.0 %

API Name

RANGER_RMS_RANGER_RMS_SERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Ranger RMS Authentication

Description

Authentication type for the Ranger RMS. Can either be "simple" or "kerberos".

Related Name

hadoop.security.authentication

Default Value

kerberos

API Name

ranger_rms_authentication

Required

false

Ranger Service

Description

Name of the Ranger service that this Ranger RMS service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

true

ZooKeeper Service

Description

Name of the ZooKeeper service that this Ranger RMS service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

rangerrms

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for conf/hadoop-metrics2.properties

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for conf/hadoop-metrics2.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/hadoop-metrics2.properties_role_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Ranger RMS Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Ranger RMS Server Log Directory

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms-conf/ranger-rms-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-site.xml

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Advanced Configuration Snippet (Safety Valve) for ranger-rms-conf/ranger-rms-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms-conf/ranger-rms-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger RMS JWKS Provider Url

Description

Whether to suppress configuration warnings produced by the Ranger RMS JWKS Provider Url configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.auth.method.dt.params.jwks.provider-url

Required

true

Suppress Configuration Validator: Ranger RMS JWT Audiences

Description

Whether to suppress configuration warnings produced by the Ranger RMS JWT Audiences configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.auth.method.dt.params.jwt.audiences

Required

true

Suppress Configuration Validator: Ranger RMS Server TLS/SSL Keystore File Alias

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server TLS/SSL Keystore File Alias configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-rms.service.https.attrib.keystore.keyalias

Required

true

Suppress Configuration Validator: Ranger RMS Client Java Opts

Description

Whether to suppress configuration warnings produced by the Ranger RMS Client Java Opts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_client_java_opts

Required

true

Suppress Configuration Validator: Ranger RMS Hive Metastore Source Service Name

Description

Whether to suppress configuration warnings produced by the Ranger RMS Hive Metastore Source Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_source_service_name

Required

true

Suppress Configuration Validator: Ranger RMS Hive Metastore Source Service Name for Ozone

Description

Whether to suppress configuration warnings produced by the Ranger RMS Hive Metastore Source Service Name for Ozone configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_source_service_name_ozone

Required

true

Suppress Configuration Validator: Ranger RMS Hive Metastore Target Service Name

Description

Whether to suppress configuration warnings produced by the Ranger RMS Hive Metastore Target Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_hms_target_service_name

Required

true

Suppress Configuration Validator: Ranger RMS Max Heapsize

Description

Whether to suppress configuration warnings produced by the Ranger RMS Max Heapsize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_max_heap_size

Required

true

Suppress Configuration Validator: Ranger RMS HA Zookeeper ACL

Description

Whether to suppress configuration warnings produced by the Ranger RMS HA Zookeeper ACL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_acl

Required

true

Suppress Configuration Validator: Ranger RMS Server Zookeeper ACL Auth

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Zookeeper ACL Auth configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_acl_auth

Required

true

Suppress Configuration Validator: Ranger RMS Server HA Zookeeper Zkroot

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server HA Zookeeper Zkroot configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ha_zookeeper_zkroot

Required

true

Suppress Configuration Validator: Ranger RMS Server IDs

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server IDs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_ids

Required

true

Suppress Configuration Validator: Ranger RMS Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: RMS HTTP Port

Description

Whether to suppress configuration warnings produced by the RMS HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_service_http_port

Required

true

Suppress Configuration Validator: RMS HTTPS Port

Description

Whether to suppress configuration warnings produced by the RMS HTTPS Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_service_https_port

Required

true

Suppress Configuration Validator: Ranger RMS Supported Uri Scheme

Description

Whether to suppress configuration warnings produced by the Ranger RMS Supported Uri Scheme configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_supported_uri_scheme

Required

true

Suppress Configuration Validator: Ranger RMS Tomcat Work Dir

Description

Whether to suppress configuration warnings produced by the Ranger RMS Tomcat Work Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_rms_tomcat_work_dir

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Ranger RMS Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Ranger RMS Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Ranger RMS Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Ranger RMS Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Ranger RMS Server Count Validator

Description

Whether to suppress configuration warnings produced by the Ranger RMS Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_rms_server_count_validator

Required

true

Suppress Parameter Validation: Ranger RMS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger RMS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_rms_service_env_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Ranger RMS Server Health

Description

Whether to suppress the results of the Ranger RMS Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ranger_rms_ranger_rms_server_healthy

Required

true

S3 Connector Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

S3 Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

AWS_S3_service_env_safety_valve

Required

false

Default S3 Endpoint

Description

Optional, default endpoint used by CDH services accessing S3, indicating the AWS region.To see a list of valid values for this parameter please consult AWS Regions and Endpoints for S3: use one of the values listed in the 'Endpoint' column, eg. 's3.us-east-2.amazonaws.com'.When not specified the endpoint used is s3.amazonaws.com

Related Name

fs.s3a.endpoint

Default Value

API Name

s3_endpoint

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Cloud Account Name

Description

Name of an AWS account. The associated AWS keys are emitted to Hue, Impala and the Hive Metastore Server.

Related Name

Default Value

API Name

cloud_account

Required

true

Security

Credentials Protection Policy

Description

Determines a security policy for the distribution of AWS account credentials to cluster services. 'More Secure': Encrypted at all times and directly available to a limited set of services. 'Less Secure': Credentials may be in plain text in some configuration files for specific services in the cluster. When IAM profiles are used, credentials are externally managed in AWS and there are no AWS credentials in any configuration files, so this setting is not applicable.

Related Name

Default Value

SECURE

API Name

key_distribution_policy

Required

true

Suppressions

Suppress Parameter Validation: S3 Connector Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Connector Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_aws_s3_service_env_safety_valve

Required

true

Suppress Parameter Validation: Default S3 Endpoint

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default S3 Endpoint parameter.

Related Name

Default Value

false

API Name

service_config_suppression_s3_endpoint

Required

true

Suppress Configuration Validator: S3Guard CDH Validator

Description

Whether to suppress configuration warnings produced by the S3Guard CDH Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_s3guard_unsupported_cdh_validator

Required

true

Schema Registry Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/schemaregistry

API Name

client_config_root_dir

Required

true

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Schema Registry Server

Advanced

Schema Registry Server XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Schema Registry Server, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-audit.xml

Description

For advanced use only. A string to be inserted into ranger-schema-registry-audit.xml for this role only.

Related Name

Default Value

API Name

ranger-schema-registry-audit.xml_role_safety_valve

Required

false

Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-schema-registry-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-schema-registry-policymgr-ssl.xml_role_safety_valve

Required

false

Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-security.xml

Description

For advanced use only. A string to be inserted into ranger-schema-registry-security.xml for this role only.

Related Name

Default Value

API Name

ranger-schema-registry-security.xml_role_safety_valve

Required

false

Schema Registry Server Advanced Configuration Snippet (Safety Valve) for registry.yaml

Description

For advanced use only. A string to be inserted into registry.yaml for this role only.

Related Name

Default Value

API Name

registry.yaml_role_safety_valve

Required

false

Schema Registry Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SCHEMA_REGISTRY_SERVER_role_env_safety_valve

Required

false

Logs

Schema Registry Server Log Directory

Description

The log directory for log files of the role Schema Registry Server.

Related Name

log_dir

Default Value

/var/log/schemaregistry

API Name

log_dir

Required

false

Schema Registry Server Logging Threshold

Description

The minimum log level for Schema Registry Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Schema Registry Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Schema Registry Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Schema Registry Server Max Log Size

Description

The maximum size, in megabytes, per log file for Schema Registry Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

schema_registry_server_fd_thresholds

Required

false

Schema Registry Server Host Health Test

Description

When computing the overall Schema Registry Server health, consider the host's health.

Related Name

Default Value

true

API Name

schema_registry_server_host_health_enabled

Required

false

Schema Registry Server Process Health Test

Description

Enables the health test that the Schema Registry Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

schema_registry_server_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Ranger Schema Registry Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.schema-registry.policy.cache.dir

Default Value

/var/lib/schemaregistry/policy-cache

API Name

ranger.plugin.schema-registry.policy.cache.dir

Required

true

Ranger Schema Registry Service Name

Description

Schema Registry service name in Ranger. If this parameter is set to the placeholder value '{{GENERATED_RANGER_SERVICE_NAME}}', a generated service name will be used, and if necessary, created. The generated service name will refer to the name of the cluster and the name of this SchemaRegistry service. The name can consist of alphanumeric, '-' and '_' characters.

Related Name

ranger.plugin.schema-registry.service.name

Default Value

cm_schema-registry

API Name

ranger.plugin.schema-registry.service.name

Required

false

Ranger Schema Registry Manager Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/schemaregistry/audit/hdfs/spool

API Name

ranger_schemaregistry_plugin_hdfs_audit_spool_directory

Required

true

Ranger Schema Registry Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/schemaregistry/audit/solr/spool

API Name

ranger_schemaregistry_plugin_solr_audit_spool_directory

Required

true

Schema Registry Admin Port

Description

The admin port for the server.

Related Name

schema.registry.adminPort

Default Value

7789

API Name

schema.registry.adminPort

Required

true

Schema Registry Allowed Resources

Description

Allowed resources for Schema Registry.

Related Name

schema.registry.allowed.resources

Default Value

401.html, back-default.png, favicon.ico

API Name

schema.registry.allowed.resources

Required

false

Enable TLS with Oracle DB

Description

Enable TLS with Oracle as DB for Schema Registry.

Related Name

schema.registry.enable.TLS.Oracle

Default Value

false

API Name

schema.registry.enable.TLS.Oracle

Required

false

Hashing Algorithm Used For Generating Fingerprints

Description

Schema Registry hashes the schema text for performance reasons. It is important to remember that changing this value to a different algorithm will require you to manually rehash all existing fingerprints and update the database accordingly.

Related Name

schema.registry.hash.function

Default Value

MD5

API Name

schema.registry.hash.function

Required

true

Password For HTTP Proxy Server Username

Description

Password For HTTP Proxy Server Username.

Related Name

schema.registry.httpProxyPassword

Default Value

API Name

schema.registry.httpProxyPassword

Required

false

HTTP Proxy Server

Description

URL for http proxy server. Please enter it in format protocol_name://host_name:port_number.

Related Name

schema.registry.httpProxyServer

Default Value

API Name

schema.registry.httpProxyServer

Required

false

HTTP Proxy Server Availability

Description

Boolean to set if HTTP Proxy Server is available or not.

Related Name

schema.registry.httpProxyServer.available

Default Value

false

API Name

schema.registry.httpProxyServer.available

Required

false

Username For HTTP Proxy Server

Description

Username for http proxy server.

Related Name

schema.registry.httpProxyUsername

Default Value

API Name

schema.registry.httpProxyUsername

Required

false

Schema Registry Jar Storage Directory Path

Description

Jar storage directory path.

Related Name

schema.registry.jar.storage.directory.path

Default Value

/tmp/schema-registry/local-jars

API Name

schema.registry.jar.storage.directory.path

Required

false

Schema Registry Jar Storage HDFS URL

Description

URL of the directory to be used for storing jars on HDFS when HDFS is not selected as an optional dependency.

Related Name

schema.registry.jar.storage.hdfs.url

Default Value

hdfs://localhost:8020

API Name

schema.registry.jar.storage.hdfs.url

Required

false

Schema Registry Jar Storage Type

Description

Jar storage type for storing jars on the local filesystem or on HDFS. If 'hdfs' is set but HDFS is not selected as an optional dependency, please provide a value for the 'Schema Registry Jar Storage HDFS URL' property.

Related Name

schema.registry.jar.storage.type

Default Value

local

API Name

schema.registry.jar.storage.type

Required

false

Oracle TLS javax.net.ssl.keyStore

Description

Path to keystore file if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.keyStore

Default Value

API Name

schema.registry.javax.net.ssl.keyStore

Required

false

Oracle TLS javax.net.ssl.keyStorePassword

Description

KeyStorePassword if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.keyStorePassword

Default Value

API Name

schema.registry.javax.net.ssl.keyStorePassword

Required

false

Oracle TLS javax.net.ssl.keyStoreType

Description

KeyStoreType type if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.keyStoreType

Default Value

API Name

schema.registry.javax.net.ssl.keyStoreType

Required

false

Oracle TLS javax.net.ssl.trustStore

Description

Required Path to truststore file if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.trustStore

Default Value

API Name

schema.registry.javax.net.ssl.trustStore

Required

false

Oracle TLS javax.net.ssl.trustStorePassword

Description

TrustStorePassword type if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.trustStorePassword

Default Value

API Name

schema.registry.javax.net.ssl.trustStorePassword

Required

false

Oracle TLS javax.net.ssl.trustStoreType

Description

Required Truststore type if enabling TLS using Oracle DB.

Related Name

schema.registry.javax.net.ssl.trustStoreType

Default Value

API Name

schema.registry.javax.net.ssl.trustStoreType

Required

false

Java Home Path Override

Description

Java home path override for Schema Registry.

Related Name

schema.registry.jdk.home

Default Value

API Name

schema.registry.jdk.home

Required

false

Schema Registry Kerberos Name Rules

Description

Kerberos name rules for Schema Registry.

Related Name

schema.registry.kerberos.name.rules

Default Value

RULE:[2:$1@$0]([jt]t@.*EXAMPLE.COM)s/.*/$MAPRED_USER/ RULE:[2:$1@$0]([nd]n@.*EXAMPLE.COM)s/.*/$HDFS_USER/DEFAULT

API Name

schema.registry.kerberos.name.rules

Required

false

Schema Registry Kerberos Non Browser User Agents

Description

Non browser user agents if kerberos is enabled.

Related Name

schema.registry.kerberos.non.browser.user.agents

Default Value

API Name

schema.registry.kerberos.non.browser.user.agents

Required

false

Schema Registry MaxRequestHeaderSize

Description

Maximum Request Header Size for the Schema Registry, in KiB.

Related Name

schema.registry.maxRequestHeaderSize

Default Value

8

API Name

schema.registry.maxRequestHeaderSize

Required

false

Oracle TLS oracle.net.authentication_services

Description

Oracle net authentication service if enabling TLS using Oracle DB.

Related Name

schema.registry.oracle.net.authentication_services

Default Value

API Name

schema.registry.oracle.net.authentication_services

Required

false

Oracle TLS oracle.net.ssl_cipher_suites

Description

Oracle net ssl cipher suites if enabling TLS using Oracle DB e.g. SSL_DH_DSS_WITH_DES_CBC_SHA.

Related Name

schema.registry.oracle.net.ssl_cipher_suites

Default Value

API Name

schema.registry.oracle.net.ssl_cipher_suites

Required

false

Oracle TLS oracle.net.ssl_server_dn_match

Description

ORacle ssl server domain name match if enabling TLS using Oracle DB.

Related Name

schema.registry.oracle.net.ssl_server_dn_match

Default Value

true

API Name

schema.registry.oracle.net.ssl_server_dn_match

Required

false

Version of oracle.net.ssl

Description

Oracle net ssl version.

Related Name

schema.registry.oracle.net.ssl_version

Default Value

API Name

schema.registry.oracle.net.ssl_version

Required

false

Schema Registry Port

Description

The port on which server accepts connections.

Related Name

schema.registry.port

Default Value

7788

API Name

schema.registry.port

Required

true

Schema Registry Proxyuser Knox Hosts

Description

Comma separated list of IP addresses from which knox can act as a trusted proxy.

Related Name

schema.registry.proxyuser.knox.hosts

Default Value

*

API Name

schema.registry.proxyuser.knox.hosts

Required

true

Schema Registry Servlet Filter

Description

Schema Registry servlet filter class.

Related Name

schema.registry.servlet.filter

Default Value

com.hortonworks.registries.auth.server.AuthenticationFilter

API Name

schema.registry.servlet.filter

Required

true

Schema Registry Admin Port (SSL)

Description

HTTPS admin port Schema Registry node runs on when SSL is enabled.

Related Name

schema.registry.ssl.adminPort

Default Value

7791

API Name

schema.registry.ssl.adminPort

Required

false

SSL Keystore Type

Description

The keystore type. It is blank by default but required if schema registry's ssl is enabled. e.g. PKCS12 or JKS. If it is left empty then this keystore type will come from CM settings.

Related Name

schema.registry.ssl.keyStoreType

Default Value

API Name

schema.registry.ssl.keyStoreType

Required

false

Schema Registry Port (SSL)

Description

HTTPS port Schema Registry node runs on when SSL is enabled.

Related Name

schema.registry.ssl.port

Default Value

7790

API Name

schema.registry.ssl.port

Required

false

SSL TrustStore Type

Description

The truststore type. It is blank by default but required if schema registry's ssl is enabled. e.g. PKCS12 or JKS. If it is left empty then this keystore type will come from CM settings.

Related Name

schema.registry.ssl.trustStoreType

Default Value

API Name

schema.registry.ssl.trustStoreType

Required

false

SSL ValidateCerts

Description

Whether or not to validate TLS certificates before starting. If enabled, it will refuse to start with expired or otherwise invalid certificates. Note: if this is enabled, the certificate revocation method (CRLDP/OCSP) is also needed. This can be done by overriding Dropwizard configuration with Java system properties. E.g: -Ddw.server.applicationConnectors[0].enableCRLDP=true (more details at https://www.dropwizard.io/en/latest/manual/core.html)

Related Name

schema.registry.ssl.validateCerts

Default Value

false

API Name

schema.registry.ssl.validateCerts

Required

false

SSL ValidatePeers

Description

Whether or not to validate TLS peer certificates.

Related Name

schema.registry.ssl.validatePeers

Default Value

false

API Name

schema.registry.ssl.validatePeers

Required

false

Schema Registry Query Timeout

Description

Schema Registry query timeout.

Related Name

schema.registry.storage.query.timeout

Default Value

30 second(s)

API Name

schema.registry.storage.query.timeout

Required

true

Schema Registry Token Validity

Description

Kerberos token validity for Schema Registry in ms.

Related Name

schema.registry.token.validity

Default Value

36000

API Name

schema.registry.token.validity

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Schema Registry Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Schema Registry Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

schema.registry.ssl.trustStorePath

Default Value

API Name

ssl_client_truststore_location

Required

false

Schema Registry Server TLS/SSL Trust Store Password

Description

The password for the Schema Registry Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

schema.registry.ssl.trustStorePassword

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Schema Registry Server

Description

Encrypt communication between clients and Schema Registry Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl.enable

Default Value

false

API Name

ssl_enabled

Required

false

Schema Registry Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Schema Registry Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

schema.registry.ssl.keyStorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Schema Registry Server TLS/SSL Server Keystore File Password

Description

The password for the Schema Registry Server keystore file.

Related Name

schema.registry.ssl.keyStorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Schema Registry Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Schema Registry Server XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Ranger Schema Registry Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Schema Registry Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.plugin.schema-registry.policy.cache.dir

Required

true

Suppress Parameter Validation: Ranger Schema Registry Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Schema Registry Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.plugin.schema-registry.service.name

Required

true

Suppress Parameter Validation: Ranger Schema Registry Manager Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Schema Registry Manager Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_schemaregistry_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Schema Registry Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Schema Registry Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_schemaregistry_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for registry.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for registry.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_registry.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Schema Registry Admin Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Admin Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.adminport

Required

true

Suppress Parameter Validation: Schema Registry Allowed Resources

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Allowed Resources parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.allowed.resources

Required

true

Suppress Parameter Validation: Hashing Algorithm Used For Generating Fingerprints

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hashing Algorithm Used For Generating Fingerprints parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.hash.function

Required

true

Suppress Parameter Validation: Password For HTTP Proxy Server Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password For HTTP Proxy Server Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxypassword

Required

true

Suppress Parameter Validation: HTTP Proxy Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Proxy Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxyserver

Required

true

Suppress Parameter Validation: Username For HTTP Proxy Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Username For HTTP Proxy Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxyusername

Required

true

Suppress Parameter Validation: Schema Registry Jar Storage Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Jar Storage Directory Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jar.storage.directory.path

Required

true

Suppress Parameter Validation: Schema Registry Jar Storage HDFS URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Jar Storage HDFS URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jar.storage.hdfs.url

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStore

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStore parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystore

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStorePassword

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStorePassword parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystorepassword

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStoreType

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStoreType parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystoretype

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStore

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStore parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststore

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStorePassword

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStorePassword parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststorepassword

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStoreType

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStoreType parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststoretype

Required

true

Suppress Parameter Validation: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Home Path Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jdk.home

Required

true

Suppress Parameter Validation: Schema Registry Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Kerberos Name Rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.kerberos.name.rules

Required

true

Suppress Parameter Validation: Schema Registry Kerberos Non Browser User Agents

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Kerberos Non Browser User Agents parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.kerberos.non.browser.user.agents

Required

true

Suppress Parameter Validation: Schema Registry MaxRequestHeaderSize

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry MaxRequestHeaderSize parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.maxrequestheadersize

Required

true

Suppress Parameter Validation: Oracle TLS oracle.net.authentication_services

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS oracle.net.authentication_services parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.authentication_services

Required

true

Suppress Parameter Validation: Oracle TLS oracle.net.ssl_cipher_suites

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS oracle.net.ssl_cipher_suites parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.ssl_cipher_suites

Required

true

Suppress Parameter Validation: Version of oracle.net.ssl

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Version of oracle.net.ssl parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.ssl_version

Required

true

Suppress Parameter Validation: Schema Registry Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.port

Required

true

Suppress Parameter Validation: Schema Registry Proxyuser Knox Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Proxyuser Knox Hosts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.proxyuser.knox.hosts

Required

true

Suppress Parameter Validation: Schema Registry Servlet Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Servlet Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.servlet.filter

Required

true

Suppress Parameter Validation: Schema Registry Admin Port (SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Admin Port (SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.adminport

Required

true

Suppress Parameter Validation: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.keystoretype

Required

true

Suppress Parameter Validation: Schema Registry Port (SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Port (SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.port

Required

true

Suppress Parameter Validation: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL TrustStore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.truststoretype

Required

true

Suppress Parameter Validation: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL ValidateCerts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.validatecerts

Required

true

Suppress Parameter Validation: SSL ValidatePeers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL ValidatePeers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.validatepeers

Required

true

Suppress Parameter Validation: Schema Registry Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema_registry_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Schema Registry Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Schema Registry Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Schema Registry Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Schema Registry Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_schemaregistry_schema_registry_server_unexpected_exits

Required

true

Service-Wide

Advanced

Schema Registry Database JDBC Url Override

Description

Specify JDBC url override for connecting to Schema Registry database. If not specified, the JDBC url will be calculated on basis of the Schema Registry database parameters specified.

Related Name

database_jdbc_url_override

Default Value

API Name

database_jdbc_url_override

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hadoop

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

schemaregistry

API Name

process_username

Required

true

Schema Registry Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

SCHEMAREGISTRY_service_env_safety_valve

Required

false

Database

Schema Registry Database Host

Description

Hostname of the database used by Schema Registry.

Related Name

schema.registry.storage.connector.host

Default Value

localhost

API Name

database_host

Required

true

Schema Registry Database Name

Description

Name of Schema Registry database.

Related Name

schema.registry.storage.connector.name

Default Value

schemaregistry

API Name

database_name

Required

true

Schema Registry Database User Password

Description

Password for Schema Registry database.

Related Name

schema.registry.storage.connector.password

Default Value

API Name

database_password

Required

true

Schema Registry Database Port

Description

Port for Schema Registry database.

Related Name

schema.registry.storage.connector.port

Default Value

3306

API Name

database_port

Required

true

Schema Registry Database Type

Description

Database type to be used (postgres).

Related Name

schema.registry.storage.connector.type

Default Value

mysql

API Name

database_type

Required

true

Schema Registry Database User

Description

User for Schema Registry database.

Related Name

schema.registry.storage.connector.user

Default Value

schemaregistry

API Name

database_user

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Healthy Schema Registry Server Monitoring Thresholds

Description

The health test thresholds of the overall Schema Registry Server health. The check returns "Concerning" health if the percentage of "Healthy" Schema Registry Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Schema Registry Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.99 %, Critical: 49.99 %

API Name

SCHEMAREGISTRY_SCHEMA_REGISTRY_SERVER_healthy_thresholds

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Enable Kerberos Authentication with Trusted Proxy

Description

Enables Trusted proxy with Kerberos authentication for this Schema Registry service.

Related Name

enable.trusted.proxy

Default Value

true

API Name

enable.trusted.proxy

Required

false

HDFS Service

Description

Name of the HDFS service that this Schema Registry service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

false

Enable Kerberos Authentication

Description

Enables Kerberos authentication for this Schema Registry service.

Related Name

kerberos.auth.enable

Default Value

false

API Name

kerberos.auth.enable

Required

false

Ranger Service

Description

Name of the Ranger service that this Schema Registry service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

schemaregistry

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Schema Registry Server Log Directory

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Schema Registry Server XML Override

Description

Whether to suppress configuration warnings produced by the Schema Registry Server XML Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-audit.xml

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-security.xml

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for ranger-schema-registry-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-schema-registry-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Ranger Schema Registry Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Schema Registry Plugin Policy Cache Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.plugin.schema-registry.policy.cache.dir

Required

true

Suppress Configuration Validator: Ranger Schema Registry Service Name

Description

Whether to suppress configuration warnings produced by the Ranger Schema Registry Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger.plugin.schema-registry.service.name

Required

true

Suppress Configuration Validator: Ranger Schema Registry Manager Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Schema Registry Manager Plugin Audit Hdfs Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_schemaregistry_plugin_hdfs_audit_spool_directory

Required

true

Suppress Configuration Validator: Ranger Schema Registry Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the Ranger Schema Registry Plugin Audit Solr Spool Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger_schemaregistry_plugin_solr_audit_spool_directory

Required

true

Suppress Configuration Validator: Schema Registry Server Advanced Configuration Snippet (Safety Valve) for registry.yaml

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Advanced Configuration Snippet (Safety Valve) for registry.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_registry.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Schema Registry Admin Port

Description

Whether to suppress configuration warnings produced by the Schema Registry Admin Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.adminport

Required

true

Suppress Configuration Validator: Schema Registry Allowed Resources

Description

Whether to suppress configuration warnings produced by the Schema Registry Allowed Resources configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.allowed.resources

Required

true

Suppress Configuration Validator: Hashing Algorithm Used For Generating Fingerprints

Description

Whether to suppress configuration warnings produced by the Hashing Algorithm Used For Generating Fingerprints configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.hash.function

Required

true

Suppress Configuration Validator: Password For HTTP Proxy Server Username

Description

Whether to suppress configuration warnings produced by the Password For HTTP Proxy Server Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxypassword

Required

true

Suppress Configuration Validator: HTTP Proxy Server

Description

Whether to suppress configuration warnings produced by the HTTP Proxy Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxyserver

Required

true

Suppress Configuration Validator: Username For HTTP Proxy Server

Description

Whether to suppress configuration warnings produced by the Username For HTTP Proxy Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.httpproxyusername

Required

true

Suppress Configuration Validator: Schema Registry Jar Storage Directory Path

Description

Whether to suppress configuration warnings produced by the Schema Registry Jar Storage Directory Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jar.storage.directory.path

Required

true

Suppress Configuration Validator: Schema Registry Jar Storage HDFS URL

Description

Whether to suppress configuration warnings produced by the Schema Registry Jar Storage HDFS URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jar.storage.hdfs.url

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStore

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStore configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystore

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStorePassword

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStorePassword configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystorepassword

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStoreType

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStoreType configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.keystoretype

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStore

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStore configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststore

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStorePassword

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStorePassword configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststorepassword

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStoreType

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStoreType configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.javax.net.ssl.truststoretype

Required

true

Suppress Configuration Validator: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the Java Home Path Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.jdk.home

Required

true

Suppress Configuration Validator: Schema Registry Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the Schema Registry Kerberos Name Rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.kerberos.name.rules

Required

true

Suppress Configuration Validator: Schema Registry Kerberos Non Browser User Agents

Description

Whether to suppress configuration warnings produced by the Schema Registry Kerberos Non Browser User Agents configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.kerberos.non.browser.user.agents

Required

true

Suppress Configuration Validator: Schema Registry MaxRequestHeaderSize

Description

Whether to suppress configuration warnings produced by the Schema Registry MaxRequestHeaderSize configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.maxrequestheadersize

Required

true

Suppress Configuration Validator: Oracle TLS oracle.net.authentication_services

Description

Whether to suppress configuration warnings produced by the Oracle TLS oracle.net.authentication_services configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.authentication_services

Required

true

Suppress Configuration Validator: Oracle TLS oracle.net.ssl_cipher_suites

Description

Whether to suppress configuration warnings produced by the Oracle TLS oracle.net.ssl_cipher_suites configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.ssl_cipher_suites

Required

true

Suppress Configuration Validator: Version of oracle.net.ssl

Description

Whether to suppress configuration warnings produced by the Version of oracle.net.ssl configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.oracle.net.ssl_version

Required

true

Suppress Configuration Validator: Schema Registry Port

Description

Whether to suppress configuration warnings produced by the Schema Registry Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.port

Required

true

Suppress Configuration Validator: Schema Registry Proxyuser Knox Hosts

Description

Whether to suppress configuration warnings produced by the Schema Registry Proxyuser Knox Hosts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.proxyuser.knox.hosts

Required

true

Suppress Configuration Validator: Schema Registry Servlet Filter

Description

Whether to suppress configuration warnings produced by the Schema Registry Servlet Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.servlet.filter

Required

true

Suppress Configuration Validator: Schema Registry Admin Port (SSL)

Description

Whether to suppress configuration warnings produced by the Schema Registry Admin Port (SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.adminport

Required

true

Suppress Configuration Validator: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the SSL Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.keystoretype

Required

true

Suppress Configuration Validator: Schema Registry Port (SSL)

Description

Whether to suppress configuration warnings produced by the Schema Registry Port (SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.port

Required

true

Suppress Configuration Validator: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the SSL TrustStore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.truststoretype

Required

true

Suppress Configuration Validator: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the SSL ValidateCerts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.validatecerts

Required

true

Suppress Configuration Validator: SSL ValidatePeers

Description

Whether to suppress configuration warnings produced by the SSL ValidatePeers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema.registry.ssl.validatepeers

Required

true

Suppress Configuration Validator: Schema Registry Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema_registry_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Schema Registry Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Schema Registry Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Schema Registry Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Schema Registry Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Schema Registry Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Schema Registry Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Schema Registry Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Schema Registry Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Schema Registry Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database Host parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_host

Required

true

Suppress Parameter Validation: Schema Registry Database JDBC Url Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database JDBC Url Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_jdbc_url_override

Required

true

Suppress Parameter Validation: Schema Registry Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_name

Required

true

Suppress Parameter Validation: Schema Registry Database User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database User Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_password

Required

true

Suppress Parameter Validation: Schema Registry Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_port

Required

true

Suppress Parameter Validation: Schema Registry Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Database User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_user

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Schema Registry Server Count Validator

Description

Whether to suppress configuration warnings produced by the Schema Registry Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_schema_registry_server_count_validator

Required

true

Suppress Parameter Validation: Schema Registry Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_schemaregistry_service_env_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Health Test: Schema Registry Server Health

Description

Whether to suppress the results of the Schema Registry Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_schemaregistry_schema_registry_server_healthy

Required

true

Solr Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/solr

API Name

client_config_root_dir

Required

true

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

solr

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

solr

API Name

process_username

Required

true

Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-audit.xml

Description

For advanced use only, a string to be inserted into ranger-solr-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-solr-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-security.xml

Description

For advanced use only, a string to be inserted into ranger-solr-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

Solr Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

solr_core_site_safety_valve

Required

false

Solr Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

solr_env_safety_valve

Required

false

Solr Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

For advanced use only, a string to be inserted into hdfs-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

solr_hdfs_site_safety_valve

Required

false

Enable Solrd Watchdog

Description

Enable the background watchdog thread that can kill Catalina process if Solr is not responsive.

Related Name

Default Value

true

API Name

solrd_enable_watchdog

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Healthy Solr Server Monitoring Thresholds

Description

The health test thresholds of the overall Solr Server health. The check returns "Concerning" health if the percentage of "Healthy" Solr Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Solr Servers falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

solr_solr_servers_healthy_thresholds

Required

false

Other

HDFS Data Directory

Description

HDFS directory used for storage by this Solr service.

Related Name

Default Value

/solr

API Name

hdfs_data_dir

Required

true

HDFS Service

Description

Name of the HDFS service that this Search service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.solr.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.solr.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Solr service instance depends on. This config is used for enabling Ranger authorization in the Solr instance not used by Ranger.

Related Name

Default Value

API Name

ranger_service

Required

false

Solr Server for Upgrade

Description

Solr server to be used while upgrading from CDH 5 to CDH 6 or to Cloudera Runtime 7.

Related Name

Default Value

API Name

solr_server_for_upgrade

Required

false

Upgrade Backup Directory

Description

Directory on the HDFS file system that is used as the backup directory while upgrading from CDH 5 to CDH 6 or to Cloudera Runtime 7.

Related Name

Default Value

/user/solr/upgrade_backup

API Name

solr_upgrade_backup_dir

Required

false

Upgrade Metadata Directory

Description

Directory on the local file system containing the migrated configurations and metadata required while upgrading from CDH 5 to CDH 6 or to Cloudera Runtime 7. Note: This directory should be present in the Solr Server specified in 'Solr Server for Upgrade'.

Related Name

Default Value

/var/lib/upgrade/solr_config

API Name

solr_upgrade_metadata_dir

Required

true

Solrd Watchdog Timeout

Description

If Solr does not respond on its web URL within this time interval, the Catalina process is killed.

Related Name

Default Value

1 minute(s), 10 second(s)

API Name

solrd_watchdog_timeout

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Search service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

ZooKeeper Znode

Description

ZooKeeper znode used to store information about this Solr service.

Related Name

Default Value

/solr

API Name

zookeeper_znode

Required

true

Security

Enable Ranger Authorization for the Infrastructure Solr Service

Description

Enable fine-grained security using Ranger for the infrastructure (infra) Solr service. This option is only for the Solr service that the Ranger service is using (for ranger-audits, etc.). No other Solr service can or should enable this option.

Related Name

Default Value

false

API Name

enable_ranger_authorization

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

solr

API Name

kerberos_princ_name

Required

true

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

Default Value

API Name

ldap_domain

Required

false

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/solr

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/solr/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/solr/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.solr.policy.cache.dir

Default Value

/var/lib/ranger/solr/policy-cache

API Name

ranger_policy_cache_dir

Required

false

Enable LDAP Authentication

Description

When checked, LDAP-based authentication for users is enabled.

Related Name

Default Value

false

API Name

solr_enable_ldap_auth

Required

false

Solr TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Solr is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

Default Value

API Name

solr_https_keystore_file

Required

false

Solr TLS/SSL Server Keystore File Password

Description

The password for the Solr keystore file.

Related Name

solr.jetty.keystore.password

Default Value

API Name

solr_https_keystore_password

Required

false

Solr TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Solr might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

solr_https_truststore_file

Required

false

Solr TLS/SSL Trust Store Password

Description

The password for the Solr TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

solr.jetty.truststore.password

Default Value

API Name

solr_https_truststore_password

Required

false

LDAP BaseDN

Description

This parameter is useful when authenticating against a non-Active Directory server, such as OpenLDAP. When set, this parameter is used to convert the username into the LDAP Distinguished Name (DN), so that the resulting DN looks like uid=username,*this parameter*. For example, if this parameter is set to "ou=People,dc=cloudera,dc=com", and the username passed in is "mike", the resulting authentication passed to the LDAP server look like "uid=mike,ou=People,dc=cloudera,dc=com". This parameter is mutually exclusive with Active Directory Domain.

Related Name

Default Value

API Name

solr_ldap_basedn

Required

false

Enable LDAP TLS

Description

If true, attempts to establish a TLS (Transport Layer Security) connection with an LDAP server that was specified with ldap://. Not required when using an LDAP URL with prefix ldaps://, because that already specifies TLS. This option is also known as "Use StartTLS".

Related Name

Default Value

false

API Name

solr_ldap_enable_starttls

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

Default Value

API Name

solr_ldap_uri

Required

false

Solr Secure Authentication

Description

Choose the authentication mechanism used by Solr.

Related Name

Default Value

simple

API Name

solr_security_authentication

Required

false

Enable TLS/SSL for Solr

Description

Encrypt communication between clients and Solr using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)). Additional manual steps must be performed; see Enabling TLS/SSL for Solr.

Related Name

Default Value

false

API Name

solr_use_ssl

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Solr Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Solr Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Solr Admin Port

Description

Whether to suppress configuration warnings produced by the Solr Admin Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_admin_port

Required

true

Suppress Configuration Validator: Solr Data Directory

Description

Whether to suppress configuration warnings produced by the Solr Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_data_dir

Required

true

Suppress Configuration Validator: Solr HTTP Port

Description

Whether to suppress configuration warnings produced by the Solr HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_http_port

Required

true

Suppress Configuration Validator: Solr HTTPS port

Description

Whether to suppress configuration warnings produced by the Solr HTTPS port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_https_port

Required

true

Suppress Configuration Validator: Java Heap Size of Solr Server in Bytes

Description

Whether to suppress configuration warnings produced by the Java Heap Size of Solr Server in Bytes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_java_heapsize

Required

true

Suppress Configuration Validator: Java Configuration Options for Solr Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Solr Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_java_opts

Required

true

Suppress Configuration Validator: Solr Load Balancer

Description

Whether to suppress configuration warnings produced by the Solr Load Balancer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_load_balancer

Required

true

Suppress Configuration Validator: Solr Server Log Directory

Description

Whether to suppress configuration warnings produced by the Solr Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_log_dir

Required

true

Suppress Configuration Validator: Solr Plugins Directory

Description

Whether to suppress configuration warnings produced by the Solr Plugins Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_plugins_dir

Required

true

Suppress Configuration Validator: Solr Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Solr Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_solr_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: HDFS Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Data Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_data_dir

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ldap_domain

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Advanced Configuration Snippet (Safety Valve) for ranger-solr-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Solr Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_core_site_safety_valve

Required

true

Suppress Parameter Validation: Solr Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_env_safety_valve

Required

true

Suppress Parameter Validation: Solr Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Service Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_hdfs_site_safety_valve

Required

true

Suppress Parameter Validation: Solr TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_https_keystore_file

Required

true

Suppress Parameter Validation: Solr TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_https_keystore_password

Required

true

Suppress Parameter Validation: Solr TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_https_truststore_file

Required

true

Suppress Parameter Validation: Solr TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_https_truststore_password

Required

true

Suppress Parameter Validation: LDAP BaseDN

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP BaseDN parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_ldap_basedn

Required

true

Suppress Configuration Validator: LDAP TLS Validator

Description

Whether to suppress configuration warnings produced by the LDAP TLS Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_solr_ldap_tls_validator

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_ldap_uri

Required

true

Suppress Configuration Validator: LDAP Secure URI and Start TLS Validator

Description

Whether to suppress configuration warnings produced by the LDAP Secure URI and Start TLS Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_solr_ldaps_or_tls_validator

Required

true

Suppress Configuration Validator: Solr Server Count Validator

Description

Whether to suppress configuration warnings produced by the Solr Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_solr_server_count_validator

Required

true

Suppress Parameter Validation: Upgrade Backup Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Upgrade Backup Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_upgrade_backup_dir

Required

true

Suppress Parameter Validation: Upgrade Metadata Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Upgrade Metadata Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solr_upgrade_metadata_dir

Required

true

Suppress Parameter Validation: Solrd Watchdog Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solrd Watchdog Timeout parameter.

Related Name

Default Value

false

API Name

service_config_suppression_solrd_watchdog_timeout

Required

true

Suppress Parameter Validation: ZooKeeper Znode

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Znode parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_znode

Required

true

Suppress Health Test: Solr Server Health

Description

Whether to suppress the results of the Solr Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_solr_solr_servers_healthy

Required

true

Solr Server

Advanced

Solr Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Java Configuration Options for Solr Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS

API Name

solr_java_opts

Required

false

Solr Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SOLR_SERVER_role_env_safety_valve

Required

false

ZooKeeper Client Timeout

Description

The time in milliseconds a client is allowed to not talk to ZooKeeper before its session expires.

Related Name

zkClientTimeout

Default Value

15 second(s)

API Name

zookeeper_client_timeout

Required

true

Logs

Solr Server Logging Threshold

Description

The minimum log level for Solr Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Solr Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Solr Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Solr Server Max Log Size

Description

The maximum size, in megabytes, per log file for Solr Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Solr Server Log Directory

Description

Directory where Solr Server will place its log files.

Related Name

Default Value

/var/log/solr

API Name

solr_log_dir

Required

true

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Solr Server API Liveness

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather status of Solr Cores from the Solr Server with a simple API request.

Related Name

Default Value

true

API Name

solr_core_status_collection_health_enabled

Required

false

Solr Server API Liveness Request Duration

Description

The health test thresholds on the duration of the Solr Server API request.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

solr_core_status_collection_thresholds

Required

false

Solr Critical State Cores

Description

Enables the health test that checks for Solr cores in Down or Recovery Failed state on a Solr Server.

Related Name

Default Value

false

API Name

solr_critical_core_health_enabled

Required

false

Solr Critical State Cores Percentage

Description

The health test thresholds for the percentage of Solr cores in Down or Recovery Failed state on a Solr Server.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

solr_critical_core_thresholds

Required

false

Solr Recovering Cores

Description

Enables the health test that checks for Recovering Solr cores on a Solr Server.

Related Name

Default Value

false

API Name

solr_recovering_core_health_enabled

Required

false

Solr Recovering Cores Percentage

Description

The health test thresholds for the percentage of Solr cores in Recovering state on a Solr Server.

Related Name

Default Value

Warning: Any, Critical: Never

API Name

solr_recovering_core_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

solr_server_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

solr_server_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

solr_server_gc_duration_window

Required

false

Solr Server Host Health Test

Description

When computing the overall Solr Server health, consider the host's health.

Related Name

Default Value

true

API Name

solr_server_host_health_enabled

Required

false

Solr Server Process Health Test

Description

Enables the health test that the Solr Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

solr_server_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

solr_server_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

solr_server_web_metric_collection_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Solr Data Directory

Description

Directory on local file system where Solr Server keeps the configurations for collections.

Related Name

Default Value

/var/lib/solr

API Name

solr_data_dir

Required

true

Graceful Shutdown Timeout

Description

Timeout (in seconds) for graceful shutdown of this Solr server. Once this timeout is reached, Solr server is abruptly shutdown. A value of 0 means no timeout.

Related Name

Default Value

3 minute(s)

API Name

solr_graceful_stop_timeout

Required

false

Solr Load Balancer

Description

Address of the load balancer, specified in host:port format.

Related Name

Default Value

API Name

solr_load_balancer

Required

false

Solr Plugins Directory

Description

Directory on local file system where Solr Server can find additional JARs. This directory is not monitored for changes during the lifetime of a solr server, and a restart is required to read any updates to the directory contents.

Related Name

Default Value

API Name

solr_plugins_dir

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Solr Max Connector Threads

Description

The maximum number of request processing threads to be created by Solr server, which determines the maximum number of simultaneous requests that can be handled.

Related Name

Default Value

10000

API Name

solr_max_connector_thread

Required

true

Ports and Addresses

Solr Admin Port

Description

Admin port of the Solr Server.

Related Name

Default Value

8984

API Name

solr_admin_port

Required

true

Solr HTTP Port

Description

HTTP port of Solr Server.

Related Name

solr_http_port

Default Value

8983

API Name

solr_http_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

HDFS Block Cache Blocks per Slab

Description

Number of blocks per cache slab. The size of the cache is 8 KB (the block size) times the number of blocks per slab times the number of slabs.

Related Name

solr.hdfs.blockcache.blocksperbank

Default Value

16384

API Name

solr_hdfs_blockcache_blocksperbank

Required

true

HDFS Block Cache Off-Heap Memory

Description

Use off-heap memory when caching HDFS blocks in Solr.

Related Name

solr.hdfs.blockcache.direct.memory.allocation

Default Value

true

API Name

solr_hdfs_blockcache_direct_memory_allocation

Required

true

HDFS Block Cache

Description

Enable caching of HDFS blocks in Solr. There is one block cache per Solr collection. configured to use off-heap memory, Maximum Off-Heap Memory must be set high enough to account for all block caches.

Related Name

solr.hdfs.blockcache.enabled

Default Value

true

API Name

solr_hdfs_blockcache_enabled

Required

true

HDFS Block Cache Number of Slabs

Description

Number of slabs per block cache. The size of the cache is 8 KB (the block size) times the number of blocks per slab times the number of slabs.

Related Name

solr.hdfs.blockcache.slab.count

Default Value

1

API Name

solr_hdfs_blockcache_slab_count

Required

true

Java Direct Memory Size of Solr Server in Bytes

Description

Maximum amount of off-heap memory in bytes that may be allocated by the Java process. Passed to Java -XX:MaxDirectMemorySize. If unset, defaults to the size of the heap.

Related Name

Default Value

1 GiB

API Name

solr_java_direct_memory_size

Required

false

Java Heap Size of Solr Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

solr_java_heapsize

Required

false

Security

Solr HTTPS port

Description

HTTPS port of Solr Server.

Related Name

solr_https_port

Default Value

8985

API Name

solr_https_port

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Solr Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Solr Admin Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Admin Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_admin_port

Required

true

Suppress Parameter Validation: Solr Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_data_dir

Required

true

Suppress Parameter Validation: Solr HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_http_port

Required

true

Suppress Parameter Validation: Solr HTTPS port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr HTTPS port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_https_port

Required

true

Suppress Parameter Validation: Java Heap Size of Solr Server in Bytes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of Solr Server in Bytes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_java_heapsize

Required

true

Suppress Parameter Validation: Java Configuration Options for Solr Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Solr Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_java_opts

Required

true

Suppress Parameter Validation: Solr Load Balancer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Load Balancer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_load_balancer

Required

true

Suppress Parameter Validation: Solr Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_log_dir

Required

true

Suppress Parameter Validation: Solr Plugins Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Plugins Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_plugins_dir

Required

true

Suppress Parameter Validation: Solr Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Solr Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_solr_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Solr Server API Liveness

Description

Whether to suppress the results of the Solr Server API Liveness heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_core_status_collection_health

Required

true

Suppress Health Test: Solr Server Critical State Cores

Description

Whether to suppress the results of the Solr Server Critical State Cores heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_critical_cores_health

Required

true

Suppress Health Test: Solr Server Recovering Cores

Description

Whether to suppress the results of the Solr Server Recovering Cores heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_recovering_cores_health

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_solr_server_web_metric_collection

Required

true

Spark Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/spark

API Name

client_config_root_dir

Required

true

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf

Description

For advanced use only, a string to be inserted into the client configuration for spark-conf/spark-defaults.conf.

Related Name

Default Value

API Name

spark-conf/spark-defaults.conf_client_config_safety_valve

Required

false

Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

For advanced use only, a string to be inserted into the client configuration for spark-conf/spark-env.sh.

Related Name

Default Value

API Name

spark-conf/spark-env.sh_client_config_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

51

API Name

client_config_priority

Required

true

Spark Data Serializer

Description

Name of class implementing org.apache.spark.serializer.Serializer to use in Spark applications.

Related Name

spark.serializer

Default Value

org.apache.spark.serializer.KryoSerializer

API Name

spark_data_serializer

Required

true

Default Application Deploy Mode

Description

Which deploy mode to use by default. Can be overridden by users when launching applications.

Related Name

spark_deploy_mode

Default Value

client

API Name

spark_deploy_mode

Required

false

Caching Executor Idle Timeout

Description

When dynamic allocation is enabled, time after which idle executors with cached RDDs blocks will be stopped. By default, they're never stopped.

Related Name

spark.dynamicAllocation.cachedExecutorIdleTimeout

Default Value

API Name

spark_dynamic_allocation_cached_idle_timeout

Required

false

Enable Dynamic Allocation

Description

Enable dynamic allocation of executors in Spark applications.

Related Name

spark.dynamicAllocation.enabled

Default Value

true

API Name

spark_dynamic_allocation_enabled

Required

false

Executor Idle Timeout

Description

When dynamic allocation is enabled, time after which idle executors will be stopped.

Related Name

spark.dynamicAllocation.executorIdleTimeout

Default Value

1 minute(s)

API Name

spark_dynamic_allocation_idle_timeout

Required

false

Initial Executor Count

Description

When dynamic allocation is enabled, number of executors to allocate when the application starts. By default, this is the same value as the minimum number of executors.

Related Name

spark.dynamicAllocation.initialExecutors

Default Value

API Name

spark_dynamic_allocation_initial_executors

Required

false

Maximum Executor Count

Description

When dynamic allocation is enabled, maximum number of executors to allocate. By default, Spark relies on YARN to control the maximum number of executors for the application.

Related Name

spark.dynamicAllocation.maxExecutors

Default Value

API Name

spark_dynamic_allocation_max_executors

Required

false

Minimum Executor Count

Description

When dynamic allocation is enabled, minimum number of executors to keep alive while the application is running.

Related Name

spark.dynamicAllocation.minExecutors

Default Value

0

API Name

spark_dynamic_allocation_min_executors

Required

false

Scheduler Backlog Timeout

Description

When dynamic allocation is enabled, timeout before requesting new executors when there are backlogged tasks.

Related Name

spark.dynamicAllocation.schedulerBacklogTimeout

Default Value

1 second(s)

API Name

spark_dynamic_allocation_scheduler_backlog_timeout

Required

false

Sustained Scheduler Backlog Timeout

Description

When dynamic allocation is enabled, timeout before requesting new executors after the initial backlog timeout has already expired. By default this is the same value as the initial backlog timeout.

Related Name

spark.dynamicAllocation.sustainedSchedulerBacklogTimeout

Default Value

API Name

spark_dynamic_allocation_sustained_scheduler_backlog_timeout

Required

false

Shell Logging Threshold

Description

The minimum log level for the Spark shell.

Related Name

spark_gateway_shell_logging_threshold

Default Value

WARN

API Name

spark_gateway_shell_logging_threshold

Required

true

Enable Kill From UI

Description

Whether to allow users to kill running stages from the Spark Web UI.

Related Name

spark.ui.killEnabled

Default Value

true

API Name

spark_gateway_ui_kill_enabled

Required

true

Enable History

Description

Write Spark application history logs to HDFS.

Related Name

spark.eventLog.enabled

Default Value

true

API Name

spark_history_enabled

Required

false

Enable I/O Encryption

Description

Whether to encrypt temporary shuffle and cache files stored by Spark on the local disks.

Related Name

spark.io.encryption.enabled

Default Value

false

API Name

spark_io_encryption_enabled

Required

false

Enable Spark Lineage

Description

Whether to enable spark lineage support. If enabled, spark lineage is sent to Atlas.

Related Name

spark.lineage.enabled

Default Value

true

API Name

spark_lineage_enabled

Required

false

Enable Network Encryption

Description

Whether to encrypt communication between Spark processes belonging to the same application. Requires authentication (spark.authenticate) to be enabled.

Related Name

spark.network.crypto.enabled

Default Value

false

API Name

spark_network_encryption_enabled

Required

false

Enable Optimized S3 Committers

Description

Whether use optimized committers when writing data to S3.

Related Name

spark.cloudera.s3_committers.enabled

Default Value

true

API Name

spark_optimized_s3_committers_enabled

Required

false

Extra Python Path

Description

Python library paths to add to PySpark applications.

Related Name

spark_python_path

Default Value

API Name

spark_python_path

Required

false

Enable Shuffle Service

Description

Enables the external shuffle service. The external shuffle service preserves shuffle files written by executors so that the executors can be deallocated without losing work. Must be enabled if Enable Dynamic Allocation is enabled. Recommended and enabled by default.

Related Name

spark.shuffle.service.enabled

Default Value

true

API Name

spark_shuffle_service_enabled

Required

true

Enable Spark Web UI

Description

Whether to enable the Spark Web UI on individual applications. It's recommended that the UI be disabled in secure clusters.

Related Name

spark.ui.enabled

Default Value

true

API Name

spark_ui_enabled

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-defaults.conf_client_config_safety_valve

Required

true

Suppress Parameter Validation: Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-env.sh_client_config_safety_valve

Required

true

Suppress Parameter Validation: Spark Data Serializer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Data Serializer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark_data_serializer

Required

true

Suppress Parameter Validation: Extra Python Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Extra Python Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark_python_path

Required

true

History Server

Advanced

History Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

For advanced use only. A string to be inserted into spark-conf/spark-env.sh for this role only.

Related Name

Default Value

API Name

spark-conf/spark-env.sh_role_safety_valve

Required

false

History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-history-server.conf

Description

For advanced use only. A string to be inserted into spark-conf/spark-history-server.conf for this role only.

Related Name

Default Value

API Name

spark-conf/spark-history-server.conf_role_safety_valve

Required

false

History Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SPARK_YARN_HISTORY_SERVER_role_env_safety_valve

Required

false

Logs

History Server Log Directory

Description

The log directory for log files of the role History Server.

Related Name

log_dir

Default Value

/var/log/spark

API Name

log_dir

Required

false

History Server Logging Threshold

Description

The minimum log level for History Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

History Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for History Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

History Server Max Log Size

Description

The maximum size, in megabytes, per log file for History Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following

configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.

- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

spark_yarn_history_server_fd_thresholds

Required

false

History Server Host Health Test

Description

When computing the overall History Server health, consider the host's health.

Related Name

Default Value

true

API Name

spark_yarn_history_server_host_health_enabled

Required

false

History Server Process Health Test

Description

Enables the health test that the History Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

spark_yarn_history_server_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Use Local Storage

Description

Whether to use local storage for caching application history data, which reduces memory usage and makes service restarts faster.

Related Name

enable_local_storage

Default Value

false

API Name

enable_local_storage

Required

false

Enable Event Log Cleaner

Description

Specifies whether the History Server should periodically clean up event logs from storage.

Related Name

spark.history.fs.cleaner.enabled

Default Value

true

API Name

event_log_cleaner_enabled

Required

false

Event Log Cleaner Interval

Description

How often the History Server will clean up event log files.

Related Name

spark.history.fs.cleaner.interval

Default Value

1 day(s)

API Name

event_log_cleaner_interval

Required

false

Maximum Event Log Age

Description

Specifies the maximum age of the event logs.

Related Name

spark.history.fs.cleaner.maxAge

Default Value

7 day(s)

API Name

event_log_cleaner_max_age

Required

false

Admin Users

Description

Comma-separated list of users who can view all applications when authentication is enabled.

Related Name

spark.history.ui.admin.acls

Default Value

knox

API Name

history_server_admin_users

Required

false

HDFS Polling Interval

Description

How often to poll HDFS for new applications.

Related Name

spark.history.fs.update.interval.seconds

Default Value

10 second(s)

API Name

history_server_fs_poll_interval

Required

false

Java Heap Size of History Server in Bytes

Description

Maximum size for the Java process heap memory. Passed to Java -Xmx. Measured in bytes.

Related Name

history_server_max_heapsize

Default Value

512 MiB

API Name

history_server_max_heapsize

Required

true

Retained App Count

Description

Max number of application UIs to keep in the History Server's memory. All applications will still be available, but may take longer to load if they're not in memory.

Related Name

spark.history.retainedApplications

Default Value

50

API Name

history_server_retained_apps

Required

false

Enable User Authentication

Description

Enables user authentication using SPNEGO (requires Kerberos), and enables access control to application history data.

Related Name

history_server_spnego_enabled

Default Value

false

API Name

history_server_spnego_enabled

Required

false

Local Storage Directory

Description

Directory where to keep local caches of application history data.

Related Name

spark.history.store.path

Default Value

/var/lib/spark/history

API Name

local_storage_dir

Required

false

Max Local Storage Size

Description

Approximate maximum amount of data to use in local storage for caching application history data.

Related Name

spark.history.store.maxDiskUsage

Default Value

10 GiB

API Name

local_storage_max_usage

Required

false

Enabled SSL/TLS Algorithms

Description

A comma-separated list of algorithm names to enable when TLS/SSL is enabled. By default, all algorithms supported by the JRE are enabled.

Related Name

spark.ssl.historyServer.enabledAlgorithms

Default Value

API Name

ssl_server_algorithms

Required

false

TLS/SSL Protocol

Description

The version of the TLS/SSL protocol to use when TLS/SSL is enabled.

Related Name

spark.ssl.historyServer.protocol

Default Value

TLSv1.2

API Name

ssl_server_protocol

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

History Server WebUI Port

Description

The port of the history server WebUI

Related Name

spark.history.ui.port

Default Value

18088

API Name

history_server_web_port

Required

true

TLS/SSL Port Number

Description

Port where to listen for TLS/SSL connections. HTTP connections will be redirected to this port when TLS/SSL is enabled.

Related Name

spark.ssl.historyServer.port

Default Value

18488

API Name

ssl_server_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable TLS/SSL for History Server

Description

Encrypt communication between clients and History Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

spark.ssl.historyServer.enabled

Default Value

false

API Name

ssl_enabled

Required

false

History Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when History Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

spark.ssl.historyServer.keyStore

Default Value

API Name

ssl_server_keystore_location

Required

false

History Server TLS/SSL Server Keystore File Password

Description

The password for the History Server keystore file.

Related Name

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Admin Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_history_server_admin_users

Required

true

Suppress Parameter Validation: History Server WebUI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server WebUI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_history_server_web_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Local Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Local Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_local_storage_dir

Required

true

Suppress Parameter Validation: History Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: History Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-env.sh_role_safety_valve

Required

true

Suppress Parameter Validation: History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-history-server.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-history-server.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-history-server.conf_role_safety_valve

Required

true

Suppress Parameter Validation: History Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spark_yarn_history_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Enabled SSL/TLS Algorithms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Enabled SSL/TLS Algorithms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_algorithms

Required

true

Suppress Parameter Validation: History Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: History Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: TLS/SSL Port Number

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Port Number parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_port

Required

true

Suppress Parameter Validation: TLS/SSL Protocol

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Protocol parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_protocol

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark_on_yarn_spark_yarn_history_server_unexpected_exits

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

spark

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

spark

API Name

process_username

Required

true

Spark Service Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

For advanced use only, a string to be inserted into spark-conf/spark-env.sh. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

spark-conf/spark-env.sh_service_safety_valve

Required

false

Spark Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

SPARK_ON_YARN_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

History Server Role Health Test

Description

When computing the overall SPARK_ON_YARN health, consider History Server's health

Related Name

Default Value

true

API Name

SPARK_ON_YARN_SPARK_YARN_HISTORY_SERVER_health_enabled

Required

false

Other

Atlas Service

Description

Name of the Atlas service that this Spark service instance depends on

Related Name

Default Value

API Name

atlas_service

Required

false

HBase Service

Description

Name of the HBase service that this Spark service instance depends on

Related Name

Default Value

API Name

hbase_service

Required

false

Spark Authentication

Description

Enable whether the Spark communication protocols do authentication using a shared secret.

Related Name

spark.authenticate

Default Value

false

API Name

spark_authenticate

Required

true

Spark Driver Log Location (HDFS)

Description

The location of Spark driver logs in HDFS when Spark application runs in client mode. Changing this value will not move existing logs to the new location.

Related Name

spark.driver.log.dfsDir

Default Value

/user/spark/driverLogs

API Name

spark_driver_log_dfs_dir

Required

true

Persist Driver Logs to Dfs

Description

If enabled, driver logs in YARN client mode will be persisted to the configured Spark Driver Log Location (HDFS)

Related Name

spark.driver.log.persistToDfs.enabled

Default Value

true

API Name

spark_driver_log_persist_to_dfs

Required

true

Spark History Location (HDFS)

Description

The location of Spark application history logs in HDFS. Changing this value will not move existing logs to the new location.

Related Name

spark.eventLog.dir

Default Value

/user/spark/applicationHistory

API Name

spark_history_log_dir

Required

true

Shuffle Service AES Encryption

Description

Whether to enable AES-based authentication and encryption in the shuffle service. Requires authentication to be enabled to take effect.

Related Name

spark_shuffle_aes_enabled

Default Value

true

API Name

spark_shuffle_aes_enabled

Required

true

YARN Service

Description

Name of the YARN service that this Spark service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

Ports and Addresses

Spark Shuffle Service Port

Description

The port the Spark Shuffle Service listens for fetch requests.

Related Name

spark.shuffle.service.port

Default Value

7337

API Name

spark_shuffle_service_port

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

spark

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Admin Users

Description

Whether to suppress configuration warnings produced by the Admin Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_history_server_admin_users

Required

true

Suppress Configuration Validator: History Server WebUI Port

Description

Whether to suppress configuration warnings produced by the History Server WebUI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_history_server_web_port

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Local Storage Directory

Description

Whether to suppress configuration warnings produced by the Local Storage Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_local_storage_dir

Required

true

Suppress Configuration Validator: History Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the History Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: History Server Log Directory

Description

Whether to suppress configuration warnings produced by the History Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf

Description

Whether to suppress configuration warnings produced by the Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-defaults.conf_client_config_safety_valve

Required

true

Suppress Configuration Validator: Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

Whether to suppress configuration warnings produced by the Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-env.sh_client_config_safety_valve

Required

true

Suppress Configuration Validator: History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

Whether to suppress configuration warnings produced by the History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-env.sh_role_safety_valve

Required

true

Suppress Configuration Validator: History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-history-server.conf

Description

Whether to suppress configuration warnings produced by the History Server Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-history-server.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark-conf/spark-history-server.conf_role_safety_valve

Required

true

Suppress Configuration Validator: Spark Data Serializer

Description

Whether to suppress configuration warnings produced by the Spark Data Serializer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark_data_serializer

Required

true

Suppress Configuration Validator: Extra Python Path

Description

Whether to suppress configuration warnings produced by the Extra Python Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark_python_path

Required

true

Suppress Configuration Validator: History Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the History Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spark_yarn_history_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Enabled SSL/TLS Algorithms

Description

Whether to suppress configuration warnings produced by the Enabled SSL/TLS Algorithms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_algorithms

Required

true

Suppress Configuration Validator: History Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the History Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: History Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the History Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: TLS/SSL Port Number

Description

Whether to suppress configuration warnings produced by the TLS/SSL Port Number configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_port

Required

true

Suppress Configuration Validator: TLS/SSL Protocol

Description

Whether to suppress configuration warnings produced by the TLS/SSL Protocol configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_protocol

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Spark Service Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Service Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-env.sh parameter.

Related Name

Default Value

false

API Name

service_config_suppression_spark-conf/spark-env.sh_service_safety_valve

Required

true

Suppress Parameter Validation: Spark Driver Log Location (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Driver Log Location (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_spark_driver_log_dfs_dir

Required

true

Suppress Parameter Validation: Spark History Location (HDFS)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark History Location (HDFS) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_spark_history_log_dir

Required

true

Suppress Configuration Validator: Hive Gateway for Spark Validator

Description

Whether to suppress configuration warnings produced by the Hive Gateway for Spark Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_spark_hive_gateway_validator

Required

true

Suppress Parameter Validation: Spark Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_spark_on_yarn_service_env_safety_valve

Required

true

Suppress Parameter Validation: Spark Shuffle Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spark Shuffle Service Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_spark_shuffle_service_port

Required

true

Suppress Configuration Validator: History Server Count Validator

Description

Whether to suppress configuration warnings produced by the History Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_spark_yarn_history_server_count_validator

Required

true

Suppress Health Test: History Server Health

Description

Whether to suppress the results of the History Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_spark_on_yarn_spark_on_yarn_spark_yarn_history_server_health

Required

true

SQL Stream Builder Properties in Cloudera Runtime 7.2.18

Role groups:

Materialized View Engine

Advanced

Materialized View Engine XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Materialized View Engine, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Materialized View Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

MATERIALIZED_VIEW_ENGINE_role_env_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions

and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Materialized View Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

For advanced use only. A string to be inserted into ssb-conf/application.properties for this role only.

Related Name

Default Value

API Name

ssb-conf/application.properties_role_safety_valve

Required

false

Logs

Materialized View Engine Log Directory

Description

The log directory for log files of the role Materialized View Engine.

Related Name

log.dir

Default Value

/var/log/ssb

API Name

log_dir

Required

false

Materialized View Engine Logging Threshold

Description

The minimum log level for Materialized View Engine logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Materialized View Engine Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Materialized View Engine logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Materialized View Engine Max Log Size

Description

The maximum size, in megabytes, per log file for Materialized View Engine logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

materialized_view_engine_fd_thresholds

Required

false

Materialized View Engine Host Health Test

Description

When computing the overall Materialized View Engine health, consider the host's health.

Related Name

Default Value

true

API Name

materialized_view_engine_host_health_enabled

Required

false

Materialized View Engine Process Health Test

Description

Enables the health test that the Materialized View Engine's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

materialized_view_engine_scm_health_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Materialized View Engine JVM Options

Description

Java options to start the JVM of the Materialized View Engine with.

Related Name

env_java_opts_materialized_view_engine

Default Value

API Name

env_java_opts_materialized_view_engine

Required

false

Sparing Kafka Admin Fail Fast

Description

Sparing Kafka Admin Fail Fast.

Related Name

spring.kafka.admin.fail-fast

Default Value

true

API Name

spring.kafka.admin.fail-fast

Required

true

Spring Kafka Consumer Key Deserializer

Description

Spring Kafka Consumer Key Deserializer.

Related Name

spring.kafka.consumer.key-deserializer

Default Value

org.apache.kafka.common.serialization.ByteArraySerializer

API Name

spring.kafka.consumer.key-deserializer

Required

true

Spring Kafka Consumer Value Deserializer

Description

Spring Kafka Consumer Value Deserializer.

Related Name

spring.kafka.consumer.value-deserializer

Default Value

org.apache.kafka.common.serialization.ByteArraySerializer

API Name

spring.kafka.consumer.value-deserializer

Required

true

Spring Kafka Producer Key Serializer

Description

Spring Kafka Producer Key Serializer.

Related Name

spring.kafka.producer.key-serializer

Default Value

org.apache.kafka.common.serialization.ByteArraySerializer

API Name

spring.kafka.producer.key-serializer

Required

true

Spring Kafka Producer Value Serializer

Description

Spring Kafka Producer Value Serializer.

Related Name

spring.kafka.producer.value-serializer

Default Value

org.apache.kafka.common.serialization.ByteArraySerializer

API Name

spring.kafka.producer.value-serializer

Required

true

Streaming SQL Administrators

Description

Streaming SQL Administrators. Users with Administrator privileges

Related Name

ssb.admins

Default Value

ssb

API Name

ssb.admins

Required

false

Database Password

Description

Materialized View database password

Related Name

ssb.mve.datasource.password

Default Value

API Name

ssb.mve.datasource.password

Required

true

Database URL (JDBC)

Description

Materialized View database URL. Only PostgreSQL is supported at the moment (e.g. jdbc:postgresql://host:port/database).

Related Name

ssb.mve.datasource.url

Default Value

jdbc:postgresql://<DB_HOST>:<DB_PORT>/<DB_SCHEMA_NAME>

API Name

ssb.mve.datasource.url

Required

true

Database User

Description

Materialized View database user

Related Name

ssb.mve.datasource.username

Default Value

API Name

ssb.mve.datasource.username

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Materialized View Engine Port

Description

Materialized View Engine Port.

Related Name

server.port

Default Value

18131

API Name

server.port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Materialized View Engine TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Materialized View Engine might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

server.ssl.trust-store

Default Value

API Name

ssl_client_truststore_location

Required

false

Materialized View Engine TLS/SSL Trust Store Password

Description

The password for the Materialized View Engine TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

server.ssl.trust-store-password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Materialized View Engine

Description

Encrypt communication between clients and Materialized View Engine using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

server.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Materialized View Engine TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Materialized View Engine is acting as a TLS/SSL server.

Related Name

server.ssl.key-password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Materialized View Engine TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Materialized View Engine is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

server.ssl.key-store

Default Value

API Name

ssl_server_keystore_location

Required

false

Materialized View Engine TLS/SSL Server Keystore File Password

Description

The password for the Materialized View Engine keystore file.

Related Name

server.ssl.key-store-password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Materialized View Engine JVM Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine JVM Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_env_java_opts_materialized_view_engine

Required

true

Suppress Parameter Validation: Materialized View Engine Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Materialized View Engine XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Materialized View Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_materialized_view_engine_role_env_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Materialized View Engine Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_server.port

Required

true

Suppress Parameter Validation: Spring Kafka Consumer Key Deserializer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spring Kafka Consumer Key Deserializer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.consumer.key-deserializer

Required

true

Suppress Parameter Validation: Spring Kafka Consumer Value Deserializer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spring Kafka Consumer Value Deserializer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.consumer.value-deserializer

Required

true

Suppress Parameter Validation: Spring Kafka Producer Key Serializer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spring Kafka Producer Key Serializer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.producer.key-serializer

Required

true

Suppress Parameter Validation: Spring Kafka Producer Value Serializer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Spring Kafka Producer Value Serializer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.producer.value-serializer

Required

true

Suppress Parameter Validation: Materialized View Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/application.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Streaming SQL Administrators

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Administrators parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.admins

Required

true

Suppress Parameter Validation: Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.password

Required

true

Suppress Parameter Validation: Database URL (JDBC)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database URL (JDBC) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.url

Required

true

Suppress Parameter Validation: Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.username

Required

true

Suppress Parameter Validation: Materialized View Engine TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Materialized View Engine TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Materialized View Engine TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Materialized View Engine TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Materialized View Engine TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_materialized_view_engine_unexpected_exits

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

ssb

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

ssb

API Name

process_username

Required

true

SQL Stream Builder Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

SQL_STREAM_BUILDER_service_env_safety_valve

Required

false

SQL Stream Builder Service Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

For advanced use only, a string to be inserted into ssb-conf/application.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ssb-conf/application.properties_service_safety_valve

Required

false

Database

Database Host

Description

Streaming SQL Builder database host.

Related Name

database_host

Default Value

localhost

API Name

database_host

Required

true

Database Password

Description

Streaming SQL Builder database password.

Related Name

database_password

Default Value

API Name

database_password

Required

true

Database Port

Description

Streaming SQL Builder database port

Related Name

database_port

Default Value

5432

API Name

database_port

Required

true

Database Name

Description

Streaming SQL Builder database name.

Related Name

database_schema

Default Value

eventador_admin

API Name

database_schema

Required

true

Database Type

Description

Streaming SQL Builder Database Type.

Related Name

database_type

Default Value

postgresql

API Name

database_type

Required

true

Database User

Description

Streaming SQL Builder database user.

Related Name

database_user

Default Value

eventador_admin

API Name

database_user

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

User Defined DDL Templates Directory

Description

User Defined DDL Templates Directory.

Related Name

custom_ddl_templates_dir

Default Value

/usr/share/flink-ddl-templates

API Name

custom_ddl_templates_dir

Required

false

DB Connector Jar Directory

Description

Directory that contains the db connector jars (must be present on all hosts!). The connector jars within are expected to be called '(postgresql|mysql|oracle)-connector-java.jar.'

Related Name

db_connector_jar_dir

Default Value

/usr/share/java/

API Name

db_connector_jar_dir

Required

false

Flink Service

Description

Name of the Flink service that this SQL Stream Builder service instance depends on

Related Name

Default Value

API Name

flink_service

Required

true

Flink SQL Connector Jar Directory

Description

Directory that contains extra flink connector jars.

Related Name

flink_sql_connector_jar_dir

Default Value

/usr/share/flink-connectors

API Name

flink_sql_connector_jar_dir

Required

true

Hive Service

Description

Name of the Hive service that this SQL Stream Builder service instance depends on

Related Name

Default Value

API Name

hive_service

Required

false

KAFKA Service

Description

Name of the KAFKA service that this SQL Stream Builder service instance depends on

Related Name

Default Value

API Name

kafka_service

Required

true

KNOX Service

Description

Name of the KNOX service that this SQL Stream Builder service instance depends on

Related Name

Default Value

API Name

knox_service

Required

false

Enable Kerberos Authentication

Description

Enables Kerberos authentication for Streaming SQL

Related Name

security.kerberos.enabled

Default Value

false

API Name

security.kerberos.enabled

Required

false

SPNEGO Keytab

Description

Kerberos keytab file with SPNEGO credentials.

Related Name

security.kerberos.spnego.keytab

Default Value

sql_stream_builder.keytab

API Name

security.kerberos.spnego.keytab

Required

false

SSB Keytab

Description

Kerberos keytab file with SSB credentials.

Related Name

security.kerberos.ssb.keytab

Default Value

sql_stream_builder.keytab

API Name

security.kerberos.ssb.keytab

Required

false

Streaming SQL Proxy Users

Description

Streaming SQL Proxy Users. Users allowed to impersonate other users

Related Name

ssb.proxy.users

Default Value

knox

API Name

ssb.proxy.users

Required

false

StreamBuilder Jar Storage Directory

Description

Directory where the repackaged streambuilder jars will be stored

Related Name

streambuilder_jar_storage_dir

Default Value

/tmp/ssb-jars

API Name

streambuilder_jar_storage_dir

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

ssb

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: Admin source IPs

Description

Whether to suppress configuration warnings produced by the Admin source IPs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_admin_source_ips

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Streaming SQL Console Default Admin Password

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Default Admin Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.admin_password

Required

true

Suppress Configuration Validator: Streaming SQL Console Default Admin Username

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Default Admin Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.admin_username

Required

true

Suppress Configuration Validator: Default organization ID

Description

Whether to suppress configuration warnings produced by the Default organization ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.default_orgid

Required

true

Suppress Configuration Validator: Fernet Encryption Key

Description

Whether to suppress configuration warnings produced by the Fernet Encryption Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.keytab_fernet_key

Required

true

Suppress Configuration Validator: Yarn resource manager external URL override

Description

Whether to suppress configuration warnings produced by the Yarn resource manager external URL override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.yarn_rm_external_url

Required

true

Suppress Configuration Validator: Streaming SQL Console External Lib Path

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console External Lib Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_console.external.python.lib.path

Required

true

Suppress Configuration Validator: Steaming SQL Console Port

Description

Whether to suppress configuration warnings produced by the Steaming SQL Console Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_console.port

Required

true

Suppress Configuration Validator: Steaming SQL Console Secure Port

Description

Whether to suppress configuration warnings produced by the Steaming SQL Console Secure Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_console.secure.port

Required

true

Suppress Configuration Validator: Materialized View Engine JVM Options

Description

Whether to suppress configuration warnings produced by the Materialized View Engine JVM Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_env_java_opts_materialized_view_engine

Required

true

Suppress Configuration Validator: Streaming SQL Engine JVM Options

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine JVM Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_env_java_opts_streaming_sql_engine

Required

true

Suppress Configuration Validator: Tag

Description

Whether to suppress configuration warnings produced by the Tag configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_environment.tag

Required

true

Suppress Configuration Validator: Flask secret key

Description

Whether to suppress configuration warnings produced by the Flask secret key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flask.secret_key

Required

true

Suppress Configuration Validator: Flask secret verification key

Description

Whether to suppress configuration warnings produced by the Flask secret verification key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_flask.secret_verification_key

Required

true

Suppress Configuration Validator: GitHub client ID

Description

Whether to suppress configuration warnings produced by the GitHub client ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_github.github_client_id

Required

true

Suppress Configuration Validator: GitHub client secret

Description

Whether to suppress configuration warnings produced by the GitHub client secret configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_github.github_client_secret

Required

true

Suppress Configuration Validator: Streaming SQL Engine Log Directory

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Streaming SQL Engine XML Override

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine XML Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Configuration Validator: Materialized View Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Materialized View Engine Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_materialized_view_engine_role_env_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: Oracle RDBMS home

Description

Whether to suppress configuration warnings produced by the Oracle RDBMS home configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oracle.home

Required

true

Suppress Configuration Validator: Schema Registry Address

Description

Whether to suppress configuration warnings produced by the Schema Registry Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_registry.address

Required

true

Suppress Configuration Validator: Rest api key

Description

Whether to suppress configuration warnings produced by the Rest api key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rest_api_configuration.api_key

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Streaming SQL Engine Port

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_server.port

Required

true

Suppress Configuration Validator: Materialized View Engine External API URL

Description

Whether to suppress configuration warnings produced by the Materialized View Engine External API URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_snapper.snapper_external_url

Required

true

Suppress Configuration Validator: Streaming SQL SocketIO Queue Kafka Auto Offset Reset

Description

Whether to suppress configuration warnings produced by the Streaming SQL SocketIO Queue Kafka Auto Offset Reset configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.kafka.auto_offset_reset

Required

true

Suppress Configuration Validator: Streaming SQL SocketIO Queue SASL Kerberos Service Name

Description

Whether to suppress configuration warnings produced by the Streaming SQL SocketIO Queue SASL Kerberos Service Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.kafka.sasl_kerberos_service_name

Required

true

Suppress Configuration Validator: Streaming SQL SocketIO Queue Protocol

Description

Whether to suppress configuration warnings produced by the Streaming SQL SocketIO Queue Protocol configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.protocol

Required

true

Suppress Configuration Validator: Spring Kafka Consumer Key Deserializer

Description

Whether to suppress configuration warnings produced by the Spring Kafka Consumer Key Deserializer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.consumer.key-deserializer

Required

true

Suppress Configuration Validator: Spring Kafka Consumer Value Deserializer

Description

Whether to suppress configuration warnings produced by the Spring Kafka Consumer Value Deserializer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.consumer.value-deserializer

Required

true

Suppress Configuration Validator: Spring Kafka Producer Key Serializer

Description

Whether to suppress configuration warnings produced by the Spring Kafka Producer Key Serializer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.producer.key-serializer

Required

true

Suppress Configuration Validator: Spring Kafka Producer Value Serializer

Description

Whether to suppress configuration warnings produced by the Spring Kafka Producer Value Serializer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_spring.kafka.producer.value-serializer

Required

true

Suppress Configuration Validator: Streaming SQL Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/application.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-conf.yaml

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-conf.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/ssb-console-conf.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-logging.yaml

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-logging.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/ssb-console-logging.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Streaming SQL Administrators

Description

Whether to suppress configuration warnings produced by the Streaming SQL Administrators configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.admins

Required

true

Suppress Configuration Validator: Database Password

Description

Whether to suppress configuration warnings produced by the Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.password

Required

true

Suppress Configuration Validator: Database URL (JDBC)

Description

Whether to suppress configuration warnings produced by the Database URL (JDBC) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.url

Required

true

Suppress Configuration Validator: Database User

Description

Whether to suppress configuration warnings produced by the Database User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssb.mve.datasource.username

Required

true

Suppress Configuration Validator: Streaming SQL Engine TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Streaming SQL Engine TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Streaming SQL Console TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console TLS/SSL Server CA Certificate (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Configuration Validator: Streaming SQL Console TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Configuration Validator: Streaming SQL Engine TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Streaming SQL Engine TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Streaming SQL Engine TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Streaming SQL Console TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Configuration Validator: Streaming SQL Console TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Streaming SQL Console Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streaming_sql_console_role_env_safety_valve

Required

true

Suppress Configuration Validator: Streaming SQL Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streaming_sql_engine_role_env_safety_valve

Required

true

Suppress Configuration Validator: Superusers

Description

Whether to suppress configuration warnings produced by the Superusers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_superusers

Required

true

Suppress Parameter Validation: User Defined DDL Templates Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the User Defined DDL Templates Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_custom_ddl_templates_dir

Required

true

Suppress Parameter Validation: Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Host parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_host

Required

true

Suppress Parameter Validation: Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_password

Required

true

Suppress Parameter Validation: Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_port

Required

true

Suppress Parameter Validation: Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_schema

Required

true

Suppress Parameter Validation: Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Database User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_user

Required

true

Suppress Parameter Validation: DB Connector Jar Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DB Connector Jar Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_db_connector_jar_dir

Required

true

Suppress Parameter Validation: Flink SQL Connector Jar Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flink SQL Connector Jar Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_flink_sql_connector_jar_dir

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: Materialized View Engine Count Validator

Description

Whether to suppress configuration warnings produced by the Materialized View Engine Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_materialized_view_engine_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: SPNEGO Keytab

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SPNEGO Keytab parameter.

Related Name

Default Value

false

API Name

service_config_suppression_security.kerberos.spnego.keytab

Required

true

Suppress Parameter Validation: SSB Keytab

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSB Keytab parameter.

Related Name

Default Value

false

API Name

service_config_suppression_security.kerberos.ssb.keytab

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: SQL Stream Builder Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SQL Stream Builder Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_sql_stream_builder_service_env_safety_valve

Required

true

Suppress Parameter Validation: SQL Stream Builder Service Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SQL Stream Builder Service Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssb-conf/application.properties_service_safety_valve

Required

true

Suppress Parameter Validation: Streaming SQL Proxy Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Proxy Users parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssb.proxy.users

Required

true

Suppress Parameter Validation: StreamBuilder Jar Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the StreamBuilder Jar Storage Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streambuilder_jar_storage_dir

Required

true

Suppress Configuration Validator: Streaming SQL Console Count Validator

Description

Whether to suppress configuration warnings produced by the Streaming SQL Console Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streaming_sql_console_count_validator

Required

true

Suppress Configuration Validator: Streaming SQL Engine Count Validator

Description

Whether to suppress configuration warnings produced by the Streaming SQL Engine Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streaming_sql_engine_count_validator

Required

true

Streaming SQL Console

Advanced

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-conf.yaml

Description

For advanced use only. A string to be inserted into ssb-conf/ssb-console-conf.yaml for this role only.

Related Name

Default Value

API Name

ssb-conf/ssb-console-conf.yaml_role_safety_valve

Required

false

Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-logging.yaml

Description

For advanced use only. A string to be inserted into ssb-conf/ssb-console-logging.yaml for this role only.

Related Name

Default Value

API Name

ssb-conf/ssb-console-logging.yaml_role_safety_valve

Required

false

Streaming SQL Console Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMING_SQL_CONSOLE_role_env_safety_valve

Required

false

Logs

Streaming SQL Console Log Directory

Description

The log directory for log files of the role Streaming SQL Console.

Related Name

log_dir

Default Value

/var/log/ssb

API Name

log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more

details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streaming_sql_console_fd_thresholds

Required

false

Streaming SQL Console Host Health Test

Description

When computing the overall Streaming SQL Console health, consider the host's health.

Related Name

Default Value

true

API Name

streaming_sql_console_host_health_enabled

Required

false

Streaming SQL Console Process Health Test

Description

Enables the health test that the Streaming SQL Console's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streaming_sql_console_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Access level map admin

Description

Access level map admin.

Related Name

access_level_map.admin

Default Value

20

API Name

access_level_map.admin

Required

false

Access level map member

Description

Access level map member.

Related Name

access_level_map.member

Default Value

10

API Name

access_level_map.member

Required

false

Access level map owner

Description

Access level map owner.

Related Name

access_level_map.owner

Default Value

30

API Name

access_level_map.owner

Required

false

Access level map ReadOnly

Description

Access level map ReadOnly.

Related Name

access_level_map.readonly

Default Value

0

API Name

access_level_map.readonly

Required

false

Admin source IPs

Description

Admin source IPs.

Related Name

admin_source_ips

Default Value

API Name

admin_source_ips

Required

false

Streaming SQL Console Default Admin Password

Description

Streaming SQL Console Default Admin Password. Enforced on each Console restart.

Related Name

cloudera_env.admin_password

Default Value

******

API Name

cloudera_env.admin_password

Required

true

Streaming SQL Console Default Admin Username

Description

Streaming SQL Console Default Admin Username. Enforced on each Console restart.

Related Name

cloudera_env.admin_username

Default Value

admin

API Name

cloudera_env.admin_username

Required

true

Default organization ID

Description

Default organization ID.

Related Name

cloudera_env.default_orgid

Default Value

ffffffffffffffffffffffffffffffff

API Name

cloudera_env.default_orgid

Required

false

Enable spnego

Description

Enable spnego.

Related Name

cloudera_env.enable_spnego

Default Value

false

API Name

cloudera_env.enable_spnego

Required

false

Fernet Encryption Key

Description

Base64-encoded 32-byte Fernet key used to encrypt keytabs stored in the admin database. (Changing this key invalidates all currently unlocked keytabs).

Related Name

cloudera_env.keytab_fernet_key

Default Value

******

API Name

cloudera_env.keytab_fernet_key

Required

true

Yarn resource manager external URL override

Description

Provides an option to overwrite the YARN URLs presented to end users. This is typically used direct the end users through the Knox proxy.

Related Name

cloudera_env.yarn_rm_external_url

Default Value

API Name

cloudera_env.yarn_rm_external_url

Required

false

Streaming SQL Console External Lib Path

Description

Streaming SQL Console External Lib Path, used by dependencies we cannot ship for some specific reasons, e.g. DB connectors.

Related Name

console.external.python.lib.path

Default Value

/usr/share/python3

API Name

console.external.python.lib.path

Required

true

Deploy Enterprise

Description

Deploy Enterprise.

Related Name

deployment.enterprise

Default Value

false

API Name

deployment.enterprise

Required

false

Current deployment version

Description

Current deployment version.

Related Name

deployment_version.current

Default Value

11

API Name

deployment_version.current

Required

false

Deployment version

Description

Deployment version.

Related Name

deployment_version.projects

Default Value

10

API Name

deployment_version.projects

Required

false

Tag

Description

Tag.

Related Name

environment.tag

Default Value

prod

API Name

environment.tag

Required

false

Enable ev8s deployment

Description

Enable ev8s deployment

Related Name

ev8s_create_deployment_enabled

Default Value

true

API Name

ev8s_create_deployment_enabled

Required

false

Feature components

Description

Feature components.

Related Name

feature_flags.components

Default Value

true

API Name

feature_flags.components

Required

false

Dashboards

Description

Dashboards.

Related Name

feature_flags.dashboards

Default Value

true

API Name

feature_flags.dashboards

Required

false

Deployments

Description

Deployments.

Related Name

feature_flags.deployments

Default Value

true

API Name

feature_flags.deployments

Required

false

Enable SASL local kafka schema detection

Description

Enable SASL local kafka schema detection.

Related Name

feature_flags.enable_sasl_local_kafka_schema_detect

Default Value

true

API Name

feature_flags.enable_sasl_local_kafka_schema_detect

Required

false

Feature environments

Description

Feature environments.

Related Name

feature_flags.environments

Default Value

true

API Name

feature_flags.environments

Required

false

External Providers

Description

External providers.

Related Name

feature_flags.external_providers

Default Value

true

API Name

feature_flags.external_providers

Required

false

Flink save points

Description

Flink save points.

Related Name

feature_flags.flink_savepoints

Default Value

true

API Name

feature_flags.flink_savepoints

Required

false

Projects

Description

Projects.

Related Name

feature_flags.projects

Default Value

true

API Name

feature_flags.projects

Required

false

Registration

Description

Registration.

Related Name

feature_flags.registration

Default Value

true

API Name

feature_flags.registration

Required

false

Stream builder

Description

Stream builder.

Related Name

feature_flags.stream_builder

Default Value

true

API Name

feature_flags.stream_builder

Required

false

Stream builder functions

Description

Stream builder functions.

Related Name

feature_flags.stream_builder_functions

Default Value

true

API Name

feature_flags.stream_builder_functions

Required

false

Flask secret key

Description

Flask secret key.

Related Name

flask.secret_key

Default Value

******

API Name

flask.secret_key

Required

false

Flask secret verification key

Description

Flask secret verification key.

Related Name

flask.secret_verification_key

Default Value

******

API Name

flask.secret_verification_key

Required

false

GitHub client ID

Description

GitHub client ID.

Related Name

github.github_client_id

Default Value

API Name

github.github_client_id

Required

false

GitHub client secret

Description

GitHub client secret.

Related Name

github.github_client_secret

Default Value

API Name

github.github_client_secret

Required

false

Kerberos TGT Renewal Interval

Description

Kerberos TGT Renewal Interval.

Related Name

kt_renewer.job_frequency

Default Value

1 hour(s)

API Name

kt_renewer.job_frequency

Required

true

Steaming SQL Console Log Level

Description

Minimum log level threshold for Steaming SQL console.

Related Name

log_level

Default Value

INFO

API Name

log_level

Required

true

Oracle RDBMS home

Description

Absolute path of the Oracle Database Manager. Used only, when the 'Database Type' is set to 'Oracle'.

Related Name

oracle.home

Default Value

/opt/oracle/product/19c/dbhome_1

API Name

oracle.home

Required

false

Schema Registry Address

Description

Schema Registry rest API address for catalog

Related Name

registry.address

Default Value

API Name

registry.address

Required

false

Rest api key

Description

Rest api key.

Related Name

rest_api_configuration.api_key

Default Value

389736e15bef4fe9b3ba839a640f5eb1

API Name

rest_api_configuration.api_key

Required

false

Materialized View Engine External API URL

Description

Materialized View Engine External API URL.

Related Name

snapper.snapper_external_url

Default Value

API Name

snapper.snapper_external_url

Required

false

Steaming SQL SocketIO Queue ON/OFF Switch

Description

Steaming SQL SocketIO Queue ON/OFF Switch

Related Name

socketio.queue.enabled

Default Value

false

API Name

socketio.queue.enabled

Required

false

Streaming SQL SocketIO Queue Kafka Auto Offset Reset

Description

Kafka auto offset reset

Related Name

socketio.queue.kafka.auto_offset_reset

Default Value

smallest

API Name

socketio.queue.kafka.auto_offset_reset

Required

false

Streaming SQL SocketIO Queue SASL Kerberos Service Name

Description

SASL Kerberos service name

Related Name

socketio.queue.kafka.sasl_kerberos_service_name

Default Value

kafka

API Name

socketio.queue.kafka.sasl_kerberos_service_name

Required

false

Streaming SQL SocketIO Queue Protocol

Description

The protocol type to use for connecting to the queue (i.e. kafka, redis, etc)

Related Name

socketio.queue.protocol

Default Value

kafka

API Name

socketio.queue.protocol

Required

false

SocketIO Log Level

Description

Minimum log level threshold for SocketIO/EngineIO.

Related Name

socketio_log_level

Default Value

WARNING

API Name

socketio_log_level

Required

true

Superusers

Description

Superusers.

Related Name

superusers

Default Value

eventador_support

API Name

superusers

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Steaming SQL Console Port

Description

Steaming SQL Console Port.

Related Name

console.port

Default Value

18111

API Name

console.port

Required

true

Steaming SQL Console Secure Port

Description

Steaming SQL Console Secure Port.

Related Name

console.secure.port

Default Value

18112

API Name

console.secure.port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Streaming SQL Console TLS/SSL Certificate Trust Store File

Description

The location on disk of the trust store, in .pem format, used to confirm the authenticity of TLS/SSL servers that Streaming SQL Console might connect to. This is used when Streaming SQL Console is the client in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl_client_truststore_location

Default Value

API Name

ssl_client_truststore_location

Required

false

Enable TLS/SSL for Streaming SQL Console

Description

Encrypt communication between clients and Streaming SQL Console using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

Streaming SQL Console TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Streaming SQL Console is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

ssl_server_ca_certificate_location

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Streaming SQL Console TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Streaming SQL Console is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_server_certificate_location

Default Value

API Name

ssl_server_certificate_location

Required

false

Streaming SQL Console TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Streaming SQL Console is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

ssl_server_privatekey_location

Default Value

API Name

ssl_server_privatekey_location

Required

false

Streaming SQL Console TLS/SSL Private Key Password

Description

The password for the private key in the Streaming SQL Console TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

ssl_server_privatekey_password

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Parameter Validation: Admin source IPs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin source IPs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_admin_source_ips

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Streaming SQL Console Default Admin Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Default Admin Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.admin_password

Required

true

Suppress Parameter Validation: Streaming SQL Console Default Admin Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Default Admin Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.admin_username

Required

true

Suppress Parameter Validation: Default organization ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default organization ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.default_orgid

Required

true

Suppress Parameter Validation: Fernet Encryption Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Fernet Encryption Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.keytab_fernet_key

Required

true

Suppress Parameter Validation: Yarn resource manager external URL override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Yarn resource manager external URL override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cloudera_env.yarn_rm_external_url

Required

true

Suppress Parameter Validation: Streaming SQL Console External Lib Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console External Lib Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_console.external.python.lib.path

Required

true

Suppress Parameter Validation: Steaming SQL Console Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Steaming SQL Console Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_console.port

Required

true

Suppress Parameter Validation: Steaming SQL Console Secure Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Steaming SQL Console Secure Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_console.secure.port

Required

true

Suppress Parameter Validation: Tag

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tag parameter.

Related Name

Default Value

false

API Name

role_config_suppression_environment.tag

Required

true

Suppress Parameter Validation: Flask secret key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flask secret key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flask.secret_key

Required

true

Suppress Parameter Validation: Flask secret verification key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Flask secret verification key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_flask.secret_verification_key

Required

true

Suppress Parameter Validation: GitHub client ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the GitHub client ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_github.github_client_id

Required

true

Suppress Parameter Validation: GitHub client secret

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the GitHub client secret parameter.

Related Name

Default Value

false

API Name

role_config_suppression_github.github_client_secret

Required

true

Suppress Parameter Validation: Streaming SQL Console Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Oracle RDBMS home

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle RDBMS home parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oracle.home

Required

true

Suppress Parameter Validation: Schema Registry Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Schema Registry Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_registry.address

Required

true

Suppress Parameter Validation: Rest api key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rest api key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rest_api_configuration.api_key

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Materialized View Engine External API URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Materialized View Engine External API URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_snapper.snapper_external_url

Required

true

Suppress Parameter Validation: Streaming SQL SocketIO Queue Kafka Auto Offset Reset

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL SocketIO Queue Kafka Auto Offset Reset parameter.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.kafka.auto_offset_reset

Required

true

Suppress Parameter Validation: Streaming SQL SocketIO Queue SASL Kerberos Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL SocketIO Queue SASL Kerberos Service Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.kafka.sasl_kerberos_service_name

Required

true

Suppress Parameter Validation: Streaming SQL SocketIO Queue Protocol

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL SocketIO Queue Protocol parameter.

Related Name

Default Value

false

API Name

role_config_suppression_socketio.queue.protocol

Required

true

Suppress Parameter Validation: Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-conf.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-conf.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/ssb-console-conf.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-logging.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Advanced Configuration Snippet (Safety Valve) for ssb-conf/ssb-console-logging.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/ssb-console-logging.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Streaming SQL Console TLS/SSL Certificate Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console TLS/SSL Certificate Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Streaming SQL Console TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Streaming SQL Console TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Streaming SQL Console TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Streaming SQL Console TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Parameter Validation: Streaming SQL Console Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Console Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streaming_sql_console_role_env_safety_valve

Required

true

Suppress Parameter Validation: Superusers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Superusers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_superusers

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_console_unexpected_exits

Required

true

Streaming SQL Engine

Advanced

Streaming SQL Engine XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Streaming SQL Engine, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among

multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Streaming SQL Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

For advanced use only. A string to be inserted into ssb-conf/application.properties for this role only.

Related Name

Default Value

API Name

ssb-conf/application.properties_role_safety_valve

Required

false

Streaming SQL Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMING_SQL_ENGINE_role_env_safety_valve

Required

false

Logs

Streaming SQL Engine Log Directory

Description

The log directory for log files of the role Streaming SQL Engine.

Related Name

log.dir

Default Value

/var/log/ssb

API Name

log_dir

Required

false

Streaming SQL Engine Logging Threshold

Description

The minimum log level for Streaming SQL Engine logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Streaming SQL Engine Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Streaming SQL Engine logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Streaming SQL Engine Max Log Size

Description

The maximum size, in megabytes, per log file for Streaming SQL Engine logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.

- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streaming_sql_engine_fd_thresholds

Required

false

Streaming SQL Engine Host Health Test

Description

When computing the overall Streaming SQL Engine health, consider the host's health.

Related Name

Default Value

true

API Name

streaming_sql_engine_host_health_enabled

Required

false

Streaming SQL Engine Process Health Test

Description

Enables the health test that the Streaming SQL Engine's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streaming_sql_engine_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Streaming SQL Engine JVM Options

Description

Java options to start the JVM of the Streaming SQL Engine with.

Related Name

env_java_opts_streaming_sql_engine

Default Value

API Name

env_java_opts_streaming_sql_engine

Required

false

Kafka Reaper Period (minutes)

Description

Minutes between Kafka Reaper runs to delete unused internal topics

Related Name

spring.kafka.reaper.period

Default Value

60

API Name

spring.kafka.reaper.period

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Streaming SQL Engine Port

Description

Streaming SQL Engine Port.

Related Name

server.port

Default Value

18121

API Name

server.port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Streaming SQL Engine TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Streaming SQL Engine might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

server.ssl.trust-store

Default Value

API Name

ssl_client_truststore_location

Required

false

Streaming SQL Engine TLS/SSL Trust Store Password

Description

The password for the Streaming SQL Engine TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

server.ssl.trust-store-password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Streaming SQL Engine

Description

Encrypt communication between clients and Streaming SQL Engine using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

server.ssl.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Streaming SQL Engine TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Streaming SQL Engine is acting as a TLS/SSL server.

Related Name

server.ssl.key-password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Streaming SQL Engine TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Streaming SQL Engine is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

server.ssl.key-store

Default Value

API Name

ssl_server_keystore_location

Required

false

Streaming SQL Engine TLS/SSL Server Keystore File Password

Description

The password for the Streaming SQL Engine keystore file.

Related Name

server.ssl.key-store-password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user

with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Streaming SQL Engine JVM Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine JVM Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_env_java_opts_streaming_sql_engine

Required

true

Suppress Parameter Validation: Streaming SQL Engine Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Streaming SQL Engine XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Streaming SQL Engine Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_server.port

Required

true

Suppress Parameter Validation: Streaming SQL Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine Advanced Configuration Snippet (Safety Valve) for ssb-conf/application.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssb-conf/application.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Streaming SQL Engine TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Streaming SQL Engine TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Streaming SQL Engine TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Streaming SQL Engine TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Streaming SQL Engine TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Streaming SQL Engine Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streaming SQL Engine Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streaming_sql_engine_role_env_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_log_directory_free_space

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_sql_stream_builder_streaming_sql_engine_unexpected_exits

Required

true

SQOOP_CLIENT Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/sqoop

API Name

client_config_root_dir

Required

true

Gateway Advanced Configuration Snippet (Safety Valve) for cm_manager_overrides

Description

For advanced use only. A string to be inserted into cm_manager_overrides for this role only.

Related Name

Default Value

API Name

sqoop-conf/managers.d/cm_manager_overrides_client_config_safety_valve

Required

false

Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-env.sh

Description

For advanced use only. A string to be inserted into sqoop-env.sh for this role only.

Related Name

Default Value

API Name

sqoop-conf/sqoop-env.sh_client_config_safety_valve

Required

false

Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-site.xml

Description

For advanced use only. A string to be inserted into sqoop-site.xml for this role only.

Related Name

Default Value

API Name

sqoop-conf/sqoop-site.xml_client_config_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Sqoop Connection Factories

Description

A list of ManagerFactory implementations which are consulted, in order to instantiate ConnManager instances used to drive connections to databases.

Related Name

sqoop.connection.factories

Default Value

API Name

sqoop_connection_factories

Required

false

Sqoop Tool Plugins

Description

A list of ToolPlugin implementations which are consulted, in order to register SqoopTool instances which allow third-party tools to be used.

Related Name

sqoop.tool.plugins

Default Value

API Name

sqoop_tool_plugins

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Gateway Advanced Configuration Snippet (Safety Valve) for cm_manager_overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Advanced Configuration Snippet (Safety Valve) for cm_manager_overrides parameter.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/managers.d/cm_manager_overrides_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/sqoop-env.sh_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/sqoop-site.xml_client_config_safety_valve

Required

true

Suppress Parameter Validation: Sqoop Connection Factories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Sqoop Connection Factories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop_connection_factories

Required

true

Suppress Parameter Validation: Sqoop Tool Plugins

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Sqoop Tool Plugins parameter.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop_tool_plugins

Required

true

Service-Wide

Advanced

SQOOP_CLIENT Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

SQOOP_CLIENT_service_env_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Parquet Writer Implementation

Description

Configure the library used during parquet jobs for writing and reading data. Possible values: hadoop, kite (legacy).

Related Name

parquetjob.configurator.implementation

Default Value

hadoop

API Name

parquetjob.configurator.implementation

Required

false

Sqoop Decimal Padding

Description

Enables padding for fixed point number types (decimal, number, numeric) in case of Avro and Parquet imports.

Related Name

sqoop.avro.decimal_padding.enable

Default Value

true

API Name

sqoop.avro.decimal_padding.enable

Required

false

Default Precision for Logical Types

Description

Specifies the default precision for fixed point number types. This value is only used if the precision was not specified in the source table.

Related Name

sqoop.avro.logical_types.decimal.default.precision

Default Value

38

API Name

sqoop.avro.logical_types.decimal.default.precision

Required

false

Default Scale for Logical Types

Description

Default scale for fixed point number types. This value is only used if the scale was not specified in the source table.

Related Name

sqoop.avro.logical_types.decimal.default.scale

Default Value

10

API Name

sqoop.avro.logical_types.decimal.default.scale

Required

false

Enable Avro Logical Types

Description

Enables the use of logical types in avro files, so that fixed point number types are converted to decimal during an import. Fixed point number types are converted to String if this property is set to false.

Related Name

sqoop.avro.logical_types.decimal.enable

Default Value

true

API Name

sqoop.avro.logical_types.decimal.enable

Required

false

Enable Parquet Logical Types

Description

Enables the use of logical types in parquet files, so that fixed point number types are converted to decimal during an import. Fixed point number types are converted to String if this property is set to false.

Related Name

sqoop.parquet.logical_types.decimal.enable

Default Value

true

API Name

sqoop.parquet.logical_types.decimal.enable

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Gateway Advanced Configuration Snippet (Safety Valve) for cm_manager_overrides

Description

Whether to suppress configuration warnings produced by the Gateway Advanced Configuration Snippet (Safety Valve) for cm_manager_overrides configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/managers.d/cm_manager_overrides_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/sqoop-env.sh_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-site.xml

Description

Whether to suppress configuration warnings produced by the Gateway Advanced Configuration Snippet (Safety Valve) for sqoop-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop-conf/sqoop-site.xml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Sqoop Connection Factories

Description

Whether to suppress configuration warnings produced by the Sqoop Connection Factories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop_connection_factories

Required

true

Suppress Configuration Validator: Sqoop Tool Plugins

Description

Whether to suppress configuration warnings produced by the Sqoop Tool Plugins configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_sqoop_tool_plugins

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Parquet Writer Implementation

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Parquet Writer Implementation parameter.

Related Name

Default Value

false

API Name

service_config_suppression_parquetjob.configurator.implementation

Required

true

Suppress Parameter Validation: SQOOP_CLIENT Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SQOOP_CLIENT Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_sqoop_client_service_env_safety_valve

Required

true

Streams Messaging Manager Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

Streams Messaging Manager Database JDBC Url Override

Description

Specify JDBC url override for connecting to Streams Messaging Manager database. If not specified, the JDBC url will be calculated on basis of the Streams Messaging Manager database parameters specified.

Related Name

database_jdbc_url_override

Default Value

API Name

database_jdbc_url_override

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

streamsmsgmgr

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

streamsmsgmgr

API Name

process_username

Required

true

Streams Messaging Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

STREAMS_MESSAGING_MANAGER_service_env_safety_valve

Required

false

Database

Streams Messaging Manager Database Host

Description

Hostname of the database used by Streams Messaging Manager. If the port is non-default for your database type, use host:port notation.

Related Name

streams.messaging.manager.storage.connector.host

Default Value

localhost

API Name

smm_database_host

Required

true

Streams Messaging Manager Database Name

Description

Name of Streams Messaging Manager database.

Related Name

streams.messaging.manager.storage.connector.name

Default Value

streamsmsgmgr

API Name

smm_database_name

Required

true

Streams Messaging Manager Database User Password

Description

Password for Streams Messaging Manager database.

Related Name

streams.messaging.manager.storage.connector.password

Default Value

API Name

smm_database_password

Required

true

Streams Messaging Manager Database Port

Description

Port for Streams Messaging Manager database.

Related Name

streams.messaging.manager.storage.connector.port

Default Value

3306

API Name

smm_database_port

Required

true

Streams Messaging Manager Database Type

Description

Database type to be used (postgres).

Related Name

streams.messaging.manager.storage.connector.type

Default Value

mysql

API Name

smm_database_type

Required

true

Streams Messaging Manager Database User

Description

User for Streams Messaging Manager database.

Related Name

streams.messaging.manager.storage.connector.user

Default Value

streamsmsgmgr

API Name

smm_database_user

Required

true

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Role Health Test

Description

When computing the overall STREAMS_MESSAGING_MANAGER health, consider Streams Messaging Manager Rest Admin Server's health

Related Name

Default Value

true

API Name

STREAMS_MESSAGING_MANAGER_STREAMS_MESSAGING_MANAGER_SERVER_health_enabled

Required

false

Streams Messaging Manager UI Server Role Health Test

Description

When computing the overall STREAMS_MESSAGING_MANAGER health, consider Streams Messaging Manager UI Server's health

Related Name

Default Value

true

API Name

STREAMS_MESSAGING_MANAGER_STREAMS_MESSAGING_MANAGER_UI_health_enabled

Required

false

Other

Enable Kerberos Authentication with Trusted Proxy

Description

Enables knox as Trusted proxy with Kerberos authentication for this SMM service.

Related Name

enable.trusted.proxy

Default Value

true

API Name

enable.trusted.proxy

Required

false

Kafka Service

Description

Name of the Kafka service that this Streams Messaging Manager service instance depends on

Related Name

Default Value

API Name

kafka_service

Required

true

Enable Kerberos Authentication

Description

Enables Kerberos authentication for this Streams Messaging Manager.

Related Name

kerberos.auth.enable

Default Value

false

API Name

kerberos.auth.enable

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.kafka.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded For IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.kafka.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Streams Messaging Manager service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Ranger SMM Plugin Conf Path

Description

Staging directory for Ranger SMM Plugin Configuration. This should generally not be changed.

Related Name

ranger_smm_plugin_conf_path

Default Value

$CONF_DIR/smm-plugin

API Name

ranger_smm_plugin_conf_path

Required

true

Ranger Streams Messaging Manager Plugin Audit Hdfs Spool Directory Path

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/streams-messaging-manager/audit/hdfs/spool

API Name

ranger_smm_plugin_hdfs_audit_spool_directory

Required

true

Ranger Streams Messaging Manager Plugin Policy Cache Directory Path

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.smm.policy.cache.dir

Default Value

/var/lib/ranger/kafka/policy-cache

API Name

ranger_smm_plugin_policy_cache_directory

Required

true

Ranger Streams Messaging Manager Plugin Audit Solr Spool Directory Path

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/streams-messaging-manager/audit/solr/spool

API Name

ranger_smm_plugin_solr_audit_spool_directory

Required

true

Schema Registry Service

Description

Name of the Schema Registry service that this Streams Messaging Manager service instance depends on

Related Name

Default Value

API Name

schemaregistry_service

Required

false

Streams Messaging Manager Port

Description

The port on which server accepts connections.

Related Name

streams.messaging.manager.port

Default Value

8585

API Name

streams.messaging.manager.port

Required

true

Streams Messaging Manager port (SSL)

Description

HTTPS port Streams Messaging Manager rest server runs on when SSL is enabled.

Related Name

streams.messaging.manager.ssl.port

Default Value

8587

API Name

streams.messaging.manager.ssl.port

Required

false

STREAMS_REPLICATION_MANAGER Service

Description

Name of the STREAMS_REPLICATION_MANAGER service that this Streams Messaging Manager service instance depends on

Related Name

Default Value

API Name

streams_replication_manager_service

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this Streams Messaging Manager service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

streamsmsgmgr

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Cloudera Manager Service Monitor Host

Description

Whether to suppress configuration warnings produced by the Cloudera Manager Service Monitor Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.service.monitor.host

Required

true

Suppress Configuration Validator: Cloudera Manager Service Monitor Port

Description

Whether to suppress configuration warnings produced by the Cloudera Manager Service Monitor Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.service.monitor.port

Required

true

Suppress Configuration Validator: Cloudera Manager Metrics TrustStore Type

Description

Whether to suppress configuration warnings produced by the Cloudera Manager Metrics TrustStore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.truststore.type

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server Advanced Configuration Snippet (Safety Valve) for config.json

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server Advanced Configuration Snippet (Safety Valve) for config.json configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_config.json_role_safety_valve

Required

true

Suppress Configuration Validator: consumer.group.refresh.interval.ms

Description

Whether to suppress configuration warnings produced by the consumer.group.refresh.interval.ms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.group.refresh.interval.ms

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for env.sh

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_env.sh_role_safety_valve

Required

true

Suppress Configuration Validator: Inactive Group Timeout

Description

Whether to suppress configuration warnings produced by the Inactive Group Timeout configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_inactive.group.timeout.ms

Required

true

Suppress Configuration Validator: inactive.producer.timeout.ms

Description

Whether to suppress configuration warnings produced by the inactive.producer.timeout.ms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_inactive.producer.timeout.ms

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Kafka Connect Host

Description

Whether to suppress configuration warnings produced by the Kafka Connect Host configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.host

Required

true

Suppress Configuration Validator: Kafka Connect Plugin Sample Configuration Path

Description

Whether to suppress configuration warnings produced by the Kafka Connect Plugin Sample Configuration Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.plugin.sample.configs.path

Required

true

Suppress Configuration Validator: Kafka Connect Port

Description

Whether to suppress configuration warnings produced by the Kafka Connect Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.port

Required

true

Suppress Configuration Validator: LatencyMetricsConfig Metrics 15m Ttl Secs

Description

Whether to suppress configuration warnings produced by the LatencyMetricsConfig Metrics 15m Ttl Secs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.15m.ttl.secs

Required

true

Suppress Configuration Validator: LatencyMetricsConfig Metrics Clean Frequency ms

Description

Whether to suppress configuration warnings produced by the LatencyMetricsConfig Metrics Clean Frequency ms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.clean.frequency.ms

Required

true

Suppress Configuration Validator: Latency Metrics Data Storage Path

Description

Whether to suppress configuration warnings produced by the Latency Metrics Data Storage Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.storage

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Log Directory

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server XML Override

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server XML Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Configuration Validator: Metrics Cache Refresh Interval ms

Description

Whether to suppress configuration warnings produced by the Metrics Cache Refresh Interval ms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.cache.refresh.interval.ms

Required

true

Suppress Configuration Validator: Metrics Fetcher Class

Description

Whether to suppress configuration warnings produced by the Metrics Fetcher Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.fetcher.class

Required

true

Suppress Configuration Validator: Number of Metrics Fetcher Threads

Description

Whether to suppress configuration warnings produced by the Number of Metrics Fetcher Threads configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.fetcher.threads

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-audit.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-security.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for schema-registry-client-ssl-config.yaml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for schema-registry-client-ssl-config.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_schema-registry-client-ssl-config.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Java Heap Size of SMM

Description

Whether to suppress configuration warnings produced by the Java Heap Size of SMM configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_smm_heap_size

Required

true

Suppress Configuration Validator: SMM_JMX_OPTS

Description

Whether to suppress configuration warnings produced by the SMM_JMX_OPTS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_smm_jmx_opts

Required

true

Suppress Configuration Validator: SMM_JVM_PERF_OPTS

Description

Whether to suppress configuration warnings produced by the SMM_JVM_PERF_OPTS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_smm_jvm_perf_opts

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-config.yaml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-config.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_srm-client-config.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-ssl-config.yaml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-ssl-config.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_srm-client-ssl-config.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server TLS/SSL Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams-messaging-manager.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager Admin Port

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Admin Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.adminport

Required

true

Suppress Configuration Validator: Allow All Alert Notifications

Description

Whether to suppress configuration warnings produced by the Allow All Alert Notifications configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.allow.all.alert.notifications

Required

true

Suppress Configuration Validator: Allowed resources

Description

Whether to suppress configuration warnings produced by the Allowed resources configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.allowed.resources

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStore

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStore configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystore

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStorePassword

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStorePassword configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystorepassword

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.keyStoreType

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.keyStoreType configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystoretype

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStore

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStore configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststore

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStorePassword

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStorePassword configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststorepassword

Required

true

Suppress Configuration Validator: Oracle TLS javax.net.ssl.trustStoreType

Description

Whether to suppress configuration warnings produced by the Oracle TLS javax.net.ssl.trustStoreType configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststoretype

Required

true

Suppress Configuration Validator: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the Java Home Path Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.jdk.home

Required

true

Suppress Configuration Validator: Kafka Alert Notification Topic

Description

Whether to suppress configuration warnings produced by the Kafka Alert Notification Topic configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kafka.alert.notifications.topic

Required

true

Suppress Configuration Validator: Kafka Cache Refresh Interval ms

Description

Whether to suppress configuration warnings produced by the Kafka Cache Refresh Interval ms configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kafka.cache.refresh.interval.ms

Required

true

Suppress Configuration Validator: Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the Kerberos Name Rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kerberos.name.rules

Required

true

Suppress Configuration Validator: Kerberos Non Browser User Agents

Description

Whether to suppress configuration warnings produced by the Kerberos Non Browser User Agents configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kerberos.non.browser.user.agents

Required

true

Suppress Configuration Validator: Oracle TLS oracle.net.authentication_services

Description

Whether to suppress configuration warnings produced by the Oracle TLS oracle.net.authentication_services configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.authentication_services

Required

true

Suppress Configuration Validator: Oracle TLS oracle.net.ssl_cipher_suites

Description

Whether to suppress configuration warnings produced by the Oracle TLS oracle.net.ssl_cipher_suites configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.ssl_cipher_suites

Required

true

Suppress Configuration Validator: oracle.net.ssl_version

Description

Whether to suppress configuration warnings produced by the oracle.net.ssl_version configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.ssl_version

Required

true

Suppress Configuration Validator: Streams Messaging Manager NotifierProviders Config Classes

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager NotifierProviders Config Classes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.providerclasses

Required

true

Suppress Configuration Validator: Save Notification Read Status Per User

Description

Whether to suppress configuration warnings produced by the Save Notification Read Status Per User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.save.notification.read.status.per.user

Required

true

Suppress Configuration Validator: Servlet filter

Description

Whether to suppress configuration warnings produced by the Servlet filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.servlet.filter

Required

true

Suppress Configuration Validator: Streams Messaging Manager Admin Port (SSL)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Admin Port (SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.adminport

Required

true

Suppress Configuration Validator: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the SSL Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.keystoretype

Required

true

Suppress Configuration Validator: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the SSL TrustStore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.truststoretype

Required

true

Suppress Configuration Validator: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the SSL ValidateCerts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.validatecerts

Required

true

Suppress Configuration Validator: SSL validatePeers

Description

Whether to suppress configuration warnings produced by the SSL validatePeers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.validatepeers

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Port

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ui.port

Required

true

Suppress Configuration Validator: Streams Messaging Manager Configuration Directory

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Configuration Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.working.directory

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams_messaging_manager_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams_messaging_manager_ui_role_env_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database JDBC Url Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database JDBC Url Override parameter.

Related Name

Default Value

false

API Name

service_config_suppression_database_jdbc_url_override

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger SMM Plugin Conf Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger SMM Plugin Conf Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_smm_plugin_conf_path

Required

true

Suppress Parameter Validation: Ranger Streams Messaging Manager Plugin Audit Hdfs Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Streams Messaging Manager Plugin Audit Hdfs Spool Directory Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_smm_plugin_hdfs_audit_spool_directory

Required

true

Suppress Parameter Validation: Ranger Streams Messaging Manager Plugin Policy Cache Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Streams Messaging Manager Plugin Policy Cache Directory Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_smm_plugin_policy_cache_directory

Required

true

Suppress Parameter Validation: Ranger Streams Messaging Manager Plugin Audit Solr Spool Directory Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Streams Messaging Manager Plugin Audit Solr Spool Directory Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_smm_plugin_solr_audit_spool_directory

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database Host parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smm_database_host

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database Name parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smm_database_name

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database User Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database User Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smm_database_password

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smm_database_port

Required

true

Suppress Parameter Validation: Streams Messaging Manager Database User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Database User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smm_database_user

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streams.messaging.manager.port

Required

true

Suppress Parameter Validation: Streams Messaging Manager port (SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager port (SSL) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streams.messaging.manager.ssl.port

Required

true

Suppress Configuration Validator: Streams Messaging Manager Rest Admin Server Count Validator

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager Rest Admin Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streams_messaging_manager_server_count_validator

Required

true

Suppress Parameter Validation: Streams Messaging Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streams_messaging_manager_service_env_safety_valve

Required

true

Suppress Configuration Validator: Streams Messaging Manager UI Server Count Validator

Description

Whether to suppress configuration warnings produced by the Streams Messaging Manager UI Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streams_messaging_manager_ui_count_validator

Required

true

Suppress Health Test: Streams Messaging Manager Rest Admin Server Health

Description

Whether to suppress the results of the Streams Messaging Manager Rest Admin Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_streams_messaging_manager_streams_messaging_manager_streams_messaging_manager_server_health

Required

true

Suppress Health Test: Streams Messaging Manager UI Server Health

Description

Whether to suppress the results of the Streams Messaging Manager UI Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_streams_messaging_manager_streams_messaging_manager_streams_messaging_manager_ui_health

Required

true

Streams Messaging Manager Rest Admin Server

Advanced

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for env.sh

Description

For advanced use only. A string to be inserted into env.sh for this role only.

Related Name

Default Value

API Name

env.sh_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for Streams Messaging Manager Rest Admin Server, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-audit.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-audit.xml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-policymgr-ssl.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

For advanced use only. A string to be inserted into ranger-kafka-security.xml for this role only.

Related Name

Default Value

API Name

ranger-kafka-security.xml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for schema-registry-client-ssl-config.yaml

Description

For advanced use only. A string to be inserted into schema-registry-client-ssl-config.yaml for this role only.

Related Name

Default Value

API Name

schema-registry-client-ssl-config.yaml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-config.yaml

Description

For advanced use only. A string to be inserted into srm-client-config.yaml for this role only.

Related Name

Default Value

API Name

srm-client-config.yaml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-ssl-config.yaml

Description

For advanced use only. A string to be inserted into srm-client-ssl-config.yaml for this role only.

Related Name

Default Value

API Name

srm-client-ssl-config.yaml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml

Description

For advanced use only. A string to be inserted into streams-messaging-manager.yaml for this role only.

Related Name

Default Value

API Name

streams-messaging-manager.yaml_role_safety_valve

Required

false

Streams Messaging Manager Rest Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMS_MESSAGING_MANAGER_SERVER_role_env_safety_valve

Required

false

Logs

Streams Messaging Manager Rest Admin Server Log Directory

Description

The log directory for log files of the role Streams Messaging Manager Rest Admin Server.

Related Name

log_dir

Default Value

/var/log/streams-messaging-manager

API Name

log_dir

Required

false

Streams Messaging Manager Rest Admin Server Logging Threshold

Description

The minimum log level for Streams Messaging Manager Rest Admin Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Streams Messaging Manager Rest Admin Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Streams Messaging Manager Rest Admin Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Streams Messaging Manager Rest Admin Server Max Log Size

Description

The maximum size, in megabytes, per log file for Streams Messaging Manager Rest Admin Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streams_messaging_manager_server_fd_thresholds

Required

false

Streams Messaging Manager Rest Admin Server Host Health Test

Description

When computing the overall Streams Messaging Manager Rest Admin Server health, consider the host's health.

Related Name

Default Value

true

API Name

streams_messaging_manager_server_host_health_enabled

Required

false

Streams Messaging Manager Rest Admin Server Process Health Test

Description

Enables the health test that the Streams Messaging Manager Rest Admin Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streams_messaging_manager_server_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Cloudera Manager Service Monitor Host

Description

Host of Cloudera Manager's Service Monitor, required when the Cloudera Manager Server and Service Monitor are not on the same host.

Related Name

cm.metrics.service.monitor.host

Default Value

API Name

cm.metrics.service.monitor.host

Required

false

Cloudera Manager Service Monitor Port

Description

Port of Cloudera Manager's Service Monitor.

Related Name

cm.metrics.service.monitor.port

Default Value

9997

API Name

cm.metrics.service.monitor.port

Required

true

Cloudera Manager Metrics TrustStore Type

Description

Cloudera Manager's truststore type. If it is left empty then the keystore type will come from CM settings. If it is left empty then the keystore type will come from CM settings.

Related Name

cm.metrics.truststore.type

Default Value

API Name

cm.metrics.truststore.type

Required

false

consumer.group.refresh.interval.ms

Description

Refresh interval for consumer group's consumption.

Related Name

consumer.group.refresh.interval.ms

Default Value

60000

API Name

consumer.group.refresh.interval.ms

Required

true

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

30 second(s)

API Name

graceful_stop_timeout

Required

false

Inactive Group Timeout

Description

Timeout in ms for inactive group.

Related Name

inactive.group.timeout.ms

Default Value

1800000

API Name

inactive.group.timeout.ms

Required

true

inactive.producer.timeout.ms

Description

Timeout in ms for Inactive producer.

Related Name

inactive.producer.timeout.ms

Default Value

1800000

API Name

inactive.producer.timeout.ms

Required

true

Kafka Connect Host

Description

Kafka Connect Rest Host

Related Name

kafka.connect.host

Default Value

API Name

kafka.connect.host

Required

false

Kafka Connect Plugin Sample Configuration Path

Description

Path to the directory containing Kafka Connector Plugins' sample json config files

Related Name

kafka.connect.plugin.sample.configs.path

Default Value

/etc/kafka_connect_ext/sample-configs

API Name

kafka.connect.plugin.sample.configs.path

Required

false

Kafka Connect Port

Description

Kafka Connect Rest Port

Related Name

kafka.connect.port

Default Value

28083

API Name

kafka.connect.port

Required

false

Kafka Connect Protocol

Description

Kafka Connect Rest Protocol

Related Name

kafka.connect.protocol

Default Value

http

API Name

kafka.connect.protocol

Required

false

Enable Latency Metrics Processing

Description

To enable Latency Metrics Processing and Servicing. SMM will launch a service which continuously processes metrics received from producers and consumers and be able to provide responses to queries.

Related Name

latencyMetricsConfig.enable.latency.metrics.processing

Default Value

true

API Name

latencyMetricsConfig.enable.latency.metrics.processing

Required

true

LatencyMetricsConfig Metrics 15m Ttl Secs

Description

Determines the default TTL (Time To Live) for 15m granularity metrics (metrics are queryable in 15m).

Related Name

latencyMetricsConfig.metrics.15m.ttl.secs

Default Value

1209600

API Name

latencyMetricsConfig.metrics.15m.ttl.secs

Required

false

LatencyMetricsConfig Metrics Clean Frequency ms

Description

Frequency with which the metrics are cleaned from the above store in ms.

Related Name

latencyMetricsConfig.metrics.clean.frequency.ms

Default Value

21600000

API Name

latencyMetricsConfig.metrics.clean.frequency.ms

Required

false

Latency Metrics Data Storage Path

Description

Path to store latency metrics data.

Related Name

latencyMetricsConfig.metrics.storage

Default Value

/var/lib/streams_messaging_manager/latencymetrics/data

API Name

latencyMetricsConfig.metrics.storage

Required

false

Logger org.apache.kafka Logging Level

Description

Logger org.apache.kafka logging level.

Related Name

logging.org.apache.kafka.level

Default Value

INFO

API Name

logging.org.apache.kafka.level

Required

false

Logger smm.kafka.webservice.common Logging Level

Description

Logger smm.kafka.webservice.common logging level.

Related Name

logging.smm.kafka.webservice.common.level

Default Value

DEBUG

API Name

logging.smm.kafka.webservice.common.level

Required

false

Metrics Cache Refresh Interval ms

Description

Refresh interval for data collection from CM Metrics's Collector cache.

Related Name

metrics.cache.refresh.interval.ms

Default Value

50000

API Name

metrics.cache.refresh.interval.ms

Required

true

Metrics Fetcher Class

Description

SMM's kafka metrics fetcher class.

Related Name

metrics.fetcher.class

Default Value

com.hortonworks.smm.kafka.services.metric.cm.CMMetricsFetcher

API Name

metrics.fetcher.class

Required

true

Number of Metrics Fetcher Threads

Description

Number of metrics fetcher threads.

Related Name

metrics.fetcher.threads

Default Value

25

API Name

metrics.fetcher.threads

Required

true

Request Metrics Separately From Cloudera Manager

Description

When checked, SMM is fetching each metrics one by one from Cloudera Manager Timeseries API. By default it is grouping metrics by their attributes so API is called less times.

Related Name

request.metrics.separately

Default Value

false

API Name

request.metrics.separately

Required

false

Java Heap Size of SMM

Description

Maximum size for the SMM Java process heap memory. Passed to Java -Xmx. Measured in megabytes.

Related Name

SMM_HEAP_SIZE

Default Value

6 GiB

API Name

SMM_HEAP_SIZE

Required

false

SMM_JMX_OPTS

Description

Change parameters to setup jmxremote.

Related Name

SMM_JMX_OPTS

Default Value

-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.management.jmxremote.ssl=false

API Name

SMM_JMX_OPTS

Required

false

SMM_JVM_PERF_OPTS

Description

SMM JVM perf and gc opts.

Related Name

SMM_JVM_PERF_OPTS

Default Value

-server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -XX:+ExplicitGCInvokesConcurrent -Djava.awt.headless=true

API Name

SMM_JVM_PERF_OPTS

Required

false

Streams Messaging Manager Admin Port

Description

The admin port for the server.

Related Name

streams.messaging.manager.adminPort

Default Value

8586

API Name

streams.messaging.manager.adminPort

Required

true

AlertTopicConsumerConfig Poll Timeout ms

Description

Alert topic Consumer config poll timeout in ms.

Related Name

streams.messaging.manager.alertTopicConsumerConfig.poll.timeout.ms

Default Value

1 second(s)

API Name

streams.messaging.manager.alertTopicConsumerConfig.poll.timeout.ms

Required

false

Allow All Alert Notifications

Description

Whether to send the alert notifications periodically.

Related Name

streams.messaging.manager.allow.all.alert.notifications

Default Value

true

API Name

streams.messaging.manager.allow.all.alert.notifications

Required

false

Allowed resources

Description

Allowed resources for Streams Messaging Manager.

Related Name

streams.messaging.manager.allowed.resources

Default Value

401.html, back-default.png, favicon.ico

API Name

streams.messaging.manager.allowed.resources

Required

false

Authorization Cache Concurrency Level

Description

The number of threads that can update the authorization cache in parallel.

Related Name

streams.messaging.manager.auth.cache.concurrency.level

Default Value

4

API Name

streams.messaging.manager.auth.cache.concurrency.level

Required

false

Authorization Cache Expiration Time

Description

The expiration time for entries in the authorization cache.

Related Name

streams.messaging.manager.auth.cache.expiration.ms

Default Value

30 second(s)

API Name

streams.messaging.manager.auth.cache.expiration.ms

Required

false

Authorization Cache Maximum Number Of Cached Items

Description

Authorization cache maximum number of cached items. Setting it to zero disables the cache.

Related Name

streams.messaging.manager.auth.cache.maximum.size

Default Value

10000

API Name

streams.messaging.manager.auth.cache.maximum.size

Required

false

Enable TLS with Oracle DB

Description

Enable TLS with Oracle as DB for Schema Registry.

Related Name

streams.messaging.manager.enable.TLS.Oracle

Default Value

false

API Name

streams.messaging.manager.enable.TLS.Oracle

Required

false

Streams Messaging Manager Executor Thread Count

Description

Alerts config executor thread count.

Related Name

streams.messaging.manager.executor.thread.count

Default Value

30

API Name

streams.messaging.manager.executor.thread.count

Required

true

Streams Messaging Manager Executor Thread Pool Size

Description

NotifierProviders executor thread pool size.

Related Name

streams.messaging.manager.executor.thread.pool.size

Default Value

16

API Name

streams.messaging.manager.executor.thread.pool.size

Required

true

Oracle TLS javax.net.ssl.keyStore

Description

Path to keystore file if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.keyStore

Default Value

API Name

streams.messaging.manager.javax.net.ssl.keyStore

Required

false

Oracle TLS javax.net.ssl.keyStorePassword

Description

KeyStorePassword if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.keyStorePassword

Default Value

API Name

streams.messaging.manager.javax.net.ssl.keyStorePassword

Required

false

Oracle TLS javax.net.ssl.keyStoreType

Description

keyStoreType type if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.keyStoreType

Default Value

API Name

streams.messaging.manager.javax.net.ssl.keyStoreType

Required

false

Oracle TLS javax.net.ssl.trustStore

Description

Required Path to truststore file if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.trustStore

Default Value

API Name

streams.messaging.manager.javax.net.ssl.trustStore

Required

false

Oracle TLS javax.net.ssl.trustStorePassword

Description

TrustStorePassword type if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.trustStorePassword

Default Value

API Name

streams.messaging.manager.javax.net.ssl.trustStorePassword

Required

false

Oracle TLS javax.net.ssl.trustStoreType

Description

Required Truststore type if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.javax.net.ssl.trustStoreType

Default Value

API Name

streams.messaging.manager.javax.net.ssl.trustStoreType

Required

false

Java Home Path Override

Description

Java Home Path Override for Streams Messaging Manager

Related Name

streams.messaging.manager.jdk.home

Default Value

API Name

streams.messaging.manager.jdk.home

Required

false

Kafka Alert Notification Topic

Description

Kafka alert notification topic name.

Related Name

streams.messaging.manager.kafka.alert.notifications.topic

Default Value

__smm_alert_notifications

API Name

streams.messaging.manager.kafka.alert.notifications.topic

Required

true

Kafka Cache Refresh Interval ms

Description

SMM's cache refresh interval in ms for kafka.

Related Name

streams.messaging.manager.kafka.cache.refresh.interval.ms

Default Value

60000

API Name

streams.messaging.manager.kafka.cache.refresh.interval.ms

Required

false

Streams Messaging Manager KafkaConsumerClient Poll Timeout ms

Description

SMM's Kafka Consumer Client poll timeout in ms.

Related Name

streams.messaging.manager.kafkaConsumerClient.poll.timeout.ms

Default Value

1 second(s)

API Name

streams.messaging.manager.kafkaConsumerClient.poll.timeout.ms

Required

false

Kerberos Name Rules

Description

Kerberos name rules for Streams Messaging Manager.

Related Name

streams.messaging.manager.kerberos.name.rules

Default Value

RULE:[2:$1@$0]([jt]t@.*EXAMPLE.COM)s/.*/$MAPRED_USER/ RULE:[2:$1@$0]([nd]n@.*EXAMPLE.COM)s/.*/$HDFS_USER/DEFAULT

API Name

streams.messaging.manager.kerberos.name.rules

Required

false

Kerberos Non Browser User Agents

Description

Non browser user agents if kerberos is enabled.

Related Name

streams.messaging.manager.kerberos.non.browser.user.agents

Default Value

API Name

streams.messaging.manager.kerberos.non.browser.user.agents

Required

false

Oracle TLS oracle.net.authentication_services

Description

oracle net authentication service if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.oracle.net.authentication_services

Default Value

API Name

streams.messaging.manager.oracle.net.authentication_services

Required

false

Oracle TLS oracle.net.ssl_cipher_suites

Description

net ssl cipher suites if enabling TLS using Oracle DB e.g. SSL_DH_DSS_WITH_DES_CBC_SHA.

Related Name

streams.messaging.manager.oracle.net.ssl_cipher_suites

Default Value

API Name

streams.messaging.manager.oracle.net.ssl_cipher_suites

Required

false

Oracle TLS oracle.net.ssl_server_dn_match

Description

ssl server domain name match if enabling TLS using Oracle DB.

Related Name

streams.messaging.manager.oracle.net.ssl_server_dn_match

Default Value

true

API Name

streams.messaging.manager.oracle.net.ssl_server_dn_match

Required

false

oracle.net.ssl_version

Description

oracle net ssl version.

Related Name

streams.messaging.manager.oracle.net.ssl_version

Default Value

API Name

streams.messaging.manager.oracle.net.ssl_version

Required

false

Streams Messaging Manager NotifierProviders Config Classes

Description

NotifierProviders config classes in list format.

Related Name

streams.messaging.manager.providerClasses

Default Value

[com.hortonworks.smm.notifier.http.HttpNotifierProvider, com.hortonworks.smm.notifier.email.EmailNotifierProvider]

API Name

streams.messaging.manager.providerClasses

Required

true

Save Notification Read Status Per User

Description

Alert notification save status flag per user.

Related Name

streams.messaging.manager.save.notification.read.status.per.user

Default Value

true

API Name

streams.messaging.manager.save.notification.read.status.per.user

Required

false

Servlet filter

Description

Streams Messaging Manager servlet filter class.

Related Name

streams.messaging.manager.servlet.filter

Default Value

com.hortonworks.registries.auth.server.AuthenticationFilter

API Name

streams.messaging.manager.servlet.filter

Required

true

Streams Messaging Manager Admin Port (SSL)

Description

HTTPS admin port Streams Messaging Manager rest server runs on when SSL is enabled.

Related Name

streams.messaging.manager.ssl.adminPort

Default Value

8588

API Name

streams.messaging.manager.ssl.adminPort

Required

false

SSL Keystore Type

Description

The keystore type. Required if Streams Messaging Manager rest server's SSL is enabled. e.g. PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.

Related Name

streams.messaging.manager.ssl.keyStoreType

Default Value

API Name

streams.messaging.manager.ssl.keyStoreType

Required

false

SSL TrustStore Type

Description

The truststore type. Required if streams messaging manager's ssl is enabled. e.g. PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.

Related Name

streams.messaging.manager.ssl.trustStoreType

Default Value

API Name

streams.messaging.manager.ssl.trustStoreType

Required

false

SSL ValidateCerts

Description

Whether or not to validate TLS certificates before starting. If enabled, it will refuse to start with expired or otherwise invalid certificates. Note: if this is enabled, the certificate revocation method (CRLDP/OCSP) is also needed. This can be done by overriding Dropwizard configuration with Java system properties. E.g: -Ddw.server.applicationConnectors[0].enableCRLDP=true (more details at https://www.dropwizard.io/en/latest/manual/core.html)

Related Name

streams.messaging.manager.ssl.validateCerts

Default Value

false

API Name

streams.messaging.manager.ssl.validateCerts

Required

false

SSL validatePeers

Description

Whether or not to validate TLS peer certificates.

Related Name

streams.messaging.manager.ssl.validatePeers

Default Value

false

API Name

streams.messaging.manager.ssl.validatePeers

Required

false

Streams Messaging Manager Query Timeout

Description

Streams Messaging Manager query timeout.

Related Name

streams.messaging.manager.storage.query.timeout

Default Value

30 millisecond(s)

API Name

streams.messaging.manager.storage.query.timeout

Required

true

Token validity

Description

Kerberos token validity for Streams Messaging Manager in ms.

Related Name

streams.messaging.manager.token.validity

Default Value

36000

API Name

streams.messaging.manager.token.validity

Required

false

Streams Messaging Manager Configuration Directory

Description

Directory to Streams messaging manager additional libs, jars, isos, etc.

Related Name

streams.messaging.manager.working.directory

Default Value

/var/lib/streams_messaging_manager

API Name

streams.messaging.manager.working.directory

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Streams Messaging Manager Rest Admin Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

streams.messaging.manager.ssl.trustStorePath

Default Value

API Name

ssl_client_truststore_location

Required

false

Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store Password

Description

The password for the Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Streams Messaging Manager Rest Admin Server

Description

Encrypt communication between clients and Streams Messaging Manager Rest Admin Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl.enable

Default Value

false

API Name

ssl_enabled

Required

false

Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Streams Messaging Manager Rest Admin Server is acting as a TLS/SSL server.

Related Name

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Streams Messaging Manager Rest Admin Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

streams.messaging.manager.ssl.keyStorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Password

Description

The password for the Streams Messaging Manager Rest Admin Server keystore file.

Related Name

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Cloudera Manager Service Monitor Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Service Monitor Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.service.monitor.host

Required

true

Suppress Parameter Validation: Cloudera Manager Service Monitor Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Service Monitor Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.service.monitor.port

Required

true

Suppress Parameter Validation: Cloudera Manager Metrics TrustStore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Metrics TrustStore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_cm.metrics.truststore.type

Required

true

Suppress Parameter Validation: consumer.group.refresh.interval.ms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the consumer.group.refresh.interval.ms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_consumer.group.refresh.interval.ms

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_env.sh_role_safety_valve

Required

true

Suppress Parameter Validation: Inactive Group Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Inactive Group Timeout parameter.

Related Name

Default Value

false

API Name

role_config_suppression_inactive.group.timeout.ms

Required

true

Suppress Parameter Validation: inactive.producer.timeout.ms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the inactive.producer.timeout.ms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_inactive.producer.timeout.ms

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Kafka Connect Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Host parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.host

Required

true

Suppress Parameter Validation: Kafka Connect Plugin Sample Configuration Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Plugin Sample Configuration Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.plugin.sample.configs.path

Required

true

Suppress Parameter Validation: Kafka Connect Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Connect Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kafka.connect.port

Required

true

Suppress Parameter Validation: LatencyMetricsConfig Metrics 15m Ttl Secs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LatencyMetricsConfig Metrics 15m Ttl Secs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.15m.ttl.secs

Required

true

Suppress Parameter Validation: LatencyMetricsConfig Metrics Clean Frequency ms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LatencyMetricsConfig Metrics Clean Frequency ms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.clean.frequency.ms

Required

true

Suppress Parameter Validation: Latency Metrics Data Storage Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Latency Metrics Data Storage Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_latencymetricsconfig.metrics.storage

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Metrics Cache Refresh Interval ms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Cache Refresh Interval ms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.cache.refresh.interval.ms

Required

true

Suppress Parameter Validation: Metrics Fetcher Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Metrics Fetcher Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.fetcher.class

Required

true

Suppress Parameter Validation: Number of Metrics Fetcher Threads

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Metrics Fetcher Threads parameter.

Related Name

Default Value

false

API Name

role_config_suppression_metrics.fetcher.threads

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-audit.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-audit.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-policymgr-ssl.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for ranger-kafka-security.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ranger-kafka-security.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for schema-registry-client-ssl-config.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for schema-registry-client-ssl-config.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_schema-registry-client-ssl-config.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Java Heap Size of SMM

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Heap Size of SMM parameter.

Related Name

Default Value

false

API Name

role_config_suppression_smm_heap_size

Required

true

Suppress Parameter Validation: SMM_JMX_OPTS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SMM_JMX_OPTS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_smm_jmx_opts

Required

true

Suppress Parameter Validation: SMM_JVM_PERF_OPTS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SMM_JVM_PERF_OPTS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_smm_jvm_perf_opts

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-config.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-config.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_srm-client-config.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-ssl-config.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for srm-client-ssl-config.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_srm-client-ssl-config.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams-messaging-manager.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager Admin Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Admin Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.adminport

Required

true

Suppress Parameter Validation: Allow All Alert Notifications

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allow All Alert Notifications parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.allow.all.alert.notifications

Required

true

Suppress Parameter Validation: Allowed resources

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed resources parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.allowed.resources

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStore

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStore parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystore

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStorePassword

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStorePassword parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystorepassword

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.keyStoreType

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.keyStoreType parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.keystoretype

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStore

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStore parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststore

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStorePassword

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStorePassword parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststorepassword

Required

true

Suppress Parameter Validation: Oracle TLS javax.net.ssl.trustStoreType

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS javax.net.ssl.trustStoreType parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.javax.net.ssl.truststoretype

Required

true

Suppress Parameter Validation: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Home Path Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.jdk.home

Required

true

Suppress Parameter Validation: Kafka Alert Notification Topic

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Alert Notification Topic parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kafka.alert.notifications.topic

Required

true

Suppress Parameter Validation: Kafka Cache Refresh Interval ms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Cache Refresh Interval ms parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kafka.cache.refresh.interval.ms

Required

true

Suppress Parameter Validation: Kerberos Name Rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Name Rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kerberos.name.rules

Required

true

Suppress Parameter Validation: Kerberos Non Browser User Agents

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Non Browser User Agents parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.kerberos.non.browser.user.agents

Required

true

Suppress Parameter Validation: Oracle TLS oracle.net.authentication_services

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS oracle.net.authentication_services parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.authentication_services

Required

true

Suppress Parameter Validation: Oracle TLS oracle.net.ssl_cipher_suites

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Oracle TLS oracle.net.ssl_cipher_suites parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.ssl_cipher_suites

Required

true

Suppress Parameter Validation: oracle.net.ssl_version

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the oracle.net.ssl_version parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.oracle.net.ssl_version

Required

true

Suppress Parameter Validation: Streams Messaging Manager NotifierProviders Config Classes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager NotifierProviders Config Classes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.providerclasses

Required

true

Suppress Parameter Validation: Save Notification Read Status Per User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Save Notification Read Status Per User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.save.notification.read.status.per.user

Required

true

Suppress Parameter Validation: Servlet filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Servlet filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.servlet.filter

Required

true

Suppress Parameter Validation: Streams Messaging Manager Admin Port (SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Admin Port (SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.adminport

Required

true

Suppress Parameter Validation: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.keystoretype

Required

true

Suppress Parameter Validation: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL TrustStore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.truststoretype

Required

true

Suppress Parameter Validation: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL ValidateCerts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.validatecerts

Required

true

Suppress Parameter Validation: SSL validatePeers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL validatePeers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ssl.validatepeers

Required

true

Suppress Parameter Validation: Streams Messaging Manager Configuration Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Configuration Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.working.directory

Required

true

Suppress Parameter Validation: Streams Messaging Manager Rest Admin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager Rest Admin Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams_messaging_manager_server_role_env_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_server_unexpected_exits

Required

true

Streams Messaging Manager UI Server

Advanced

Streams Messaging Manager UI Server Advanced Configuration Snippet (Safety Valve) for config.json

Description

For advanced use only. A string to be inserted into config.json for this role only.

Related Name

Default Value

API Name

config.json_role_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Streams Messaging Manager UI Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMS_MESSAGING_MANAGER_UI_role_env_safety_valve

Required

false

Logs

Streams Messaging Manager UI Server Log Directory

Description

The log directory for log files of the role Streams Messaging Manager UI Server.

Related Name

log_dir

Default Value

/var/log/streams-messaging-manager

API Name

log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streams_messaging_manager_ui_fd_thresholds

Required

false

Streams Messaging Manager UI Server Host Health Test

Description

When computing the overall Streams Messaging Manager UI Server health, consider the host's health.

Related Name

Default Value

true

API Name

streams_messaging_manager_ui_host_health_enabled

Required

false

Streams Messaging Manager UI Server Process Health Test

Description

Enables the health test that the Streams Messaging Manager UI Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streams_messaging_manager_ui_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Graceful Shutdown Timeout

Description

The timeout in milliseconds to wait for graceful shutdown to complete.

Related Name

Default Value

30 second(s)

API Name

graceful_stop_timeout

Required

false

Streams Messaging Manager UI Port

Description

The port on which server accepts connections.

Related Name

streams.messaging.manager.ui.port

Default Value

9991

API Name

streams.messaging.manager.ui.port

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Streams Messaging Manager UI Server TLS/SSL Certificate Trust Store File

Description

The location on disk of the trust store, in .pem format, used to confirm the authenticity of TLS/SSL servers that Streams Messaging Manager UI Server might connect to. This is used when Streams Messaging Manager UI Server is the client in a TLS/SSL connection. This trust store must contain

the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

streams.messaging.manager.ui.ssl.trust.store.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Enable TLS/SSL for Streams Messaging Manager UI Server

Description

Encrypt communication between clients and Streams Messaging Manager UI Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

streams.messaging.manager.ui.ssl.enable

Default Value

false

API Name

ssl_enabled

Required

false

Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format)

Description

The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.

Related Name

streams.messaging.manager.ui.ssl.ca.cert.location

Default Value

API Name

ssl_server_ca_certificate_location

Required

false

Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format)

Description

The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

streams.messaging.manager.ui.ssl.cert.location

Default Value

API Name

ssl_server_certificate_location

Required

false

Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format)

Description

The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format.

Related Name

streams.messaging.manager.ui.ssl.private.key.location

Default Value

API Name

ssl_server_privatekey_location

Required

false

Streams Messaging Manager UI Server TLS/SSL Private Key Password

Description

The password for the private key in the Streams Messaging Manager UI Server TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.

Related Name

Default Value

API Name

ssl_server_privatekey_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server Advanced Configuration Snippet (Safety Valve) for config.json

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server Advanced Configuration Snippet (Safety Valve) for config.json parameter.

Related Name

Default Value

false

API Name

role_config_suppression_config.json_role_safety_valve

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server TLS/SSL Certificate Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server TLS/SSL Certificate Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_ca_certificate_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_certificate_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_location

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server TLS/SSL Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server TLS/SSL Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_privatekey_password

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.messaging.manager.ui.port

Required

true

Suppress Parameter Validation: Streams Messaging Manager UI Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Messaging Manager UI Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams_messaging_manager_ui_role_env_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_messaging_manager_streams_messaging_manager_ui_unexpected_exits

Required

true

Streams Replication Manager Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/streams_replication_manager

API Name

client_config_root_dir

Required

true

Streams Replication Manager Client Advanced Configuration Snippet (Safety Valve) for streams_replication_manager-conf/srm.properties

Description

For advanced use only, a string to be inserted into the client configuration for streams_replication_manager-conf/srm.properties.

Related Name

Default Value

API Name

streams_replication_manager-conf/srm.properties_client_config_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

SRM Client's Kerberos Keytab Location

Description

The path of the kerberos keytab file to be used by the SRM Client to authenticate with the co-located Kafka cluster. If left empty, the JAAS configuration of the co-located Kafka connection will not be generated.

Related Name

kerberos.keytab.location

Default Value

API Name

kerberos.keytab.location

Required

false

SRM Client's Kerberos Principal Name

Description

The kerberos principal name of the SRM Client to authenticate with the co-located Kafka cluster. If left empty, the JAAS configuration of the co-located Kafka connection will not be generated.

Related Name

kerberos.principal.name

Default Value

API Name

kerberos.principal.name

Required

false

SRM Client's Secure Storage Password

Description

Password for the secure storage that securely stores the sensitive client configurations. The default value is an empty string. If left empty, the SRM Client Secure Storage will not be created, and sensitive configuration will not be available for the client.

Related Name

securestorage.password

Default Value

API Name

securestorage.password

Required

true

Environment Variable Holding SRM Client's Secure Storage Password

Description

Name of the environment variable that stores the password for the SRM Client's secure storage.

Related Name

config.providers.secure.param.keystore.password.value

Default Value

SECURESTOREPASS

API Name

securestorage.password.variable

Required

false

SRM Client's Secure Storage Type

Description

Type of secure storage that securely stores sensitive client configurations. This must be a valid Java keystore type that supports storage of symmetric cryptographic keys.

Related Name

config.providers.secure.param.secureconfig.keystore.type

Default Value

PKCS12

API Name

securestorage.type

Required

false

SRM Client's TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when a SRM Client is authenticated as an SSL client against a Kafka cluster. If left empty, this configuration is not saved into the respective secure client configuration, preventing the use of the client keystore.

Related Name

ssl.keystore.keypassword

Default Value

API Name

ssl.keystore.keypassword

Required

false

Keystore file Location for the SRM client's TLS/SSL server

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. This path is used when an SRM Client authenticates as an SSL client against a Kafka cluster.

Related Name

ssl.keystore.location

Default Value

API Name

ssl.keystore.location

Required

false

SRM Client's TLS/SSL Server Keystore File Password

Description

The password for the SRM Client keystore file. If left empty, this config will not be saved into the respective secure client configuration, preventing the use of the Client Keystore.

Related Name

ssl.keystore.password

Default Value

API Name

ssl.keystore.password

Required

false

Security

Gateway TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Gateway might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Gateway TLS/SSL Trust Store Password

Description

The password for the Gateway TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: SRM Client's Kerberos Keytab Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's Kerberos Keytab Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos.keytab.location

Required

true

Suppress Parameter Validation: SRM Client's Kerberos Principal Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's Kerberos Principal Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos.principal.name

Required

true

Suppress Parameter Validation: SRM Client's Secure Storage Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's Secure Storage Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.password

Required

true

Suppress Parameter Validation: Environment Variable Holding SRM Client's Secure Storage Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Environment Variable Holding SRM Client's Secure Storage Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.password.variable

Required

true

Suppress Parameter Validation: SRM Client's Secure Storage Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's Secure Storage Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.type

Required

true

Suppress Parameter Validation: SRM Client's TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.keypassword

Required

true

Suppress Parameter Validation: Keystore file Location for the SRM client's TLS/SSL server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Keystore file Location for the SRM client's TLS/SSL server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.location

Required

true

Suppress Parameter Validation: SRM Client's TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Client's TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.password

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Gateway TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Streams Replication Manager Client Advanced Configuration Snippet (Safety Valve) for streams_replication_manager-conf/srm.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Client Advanced Configuration Snippet (Safety Valve) for streams_replication_manager-conf/srm.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager-conf/srm.properties_client_config_safety_valve

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

streamsrepmgr

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

streamsrepmgr

API Name

process_username

Required

true

Streams Replication Manager Service Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

For advanced use only, a string to be inserted into srm.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

srm.properties_service_safety_valve

Required

false

Streams Replication Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

STREAMS_REPLICATION_MANAGER_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Healthy SRM Driver Monitoring Thresholds

Description

The health test thresholds of the overall SRM Driver health. The check returns "Concerning" health if the percentage of "Healthy" SRM Drivers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" SRM Drivers falls below the critical threshold.

Related Name

Default Value

Warning: 94.99 %, Critical: 49.99 %

API Name

STREAMS_REPLICATION_MANAGER_STREAMS_REPLICATION_MANAGER_DRIVER_healthy_thresholds

Required

false

Healthy SRM Service Monitoring Thresholds

Description

The health test thresholds of the overall SRM Service health. The check returns "Concerning" health if the percentage of "Healthy" SRM Services falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" SRM Services falls below the critical threshold.

Related Name

Default Value

Warning: 94.99 %, Critical: 49.99 %

API Name

STREAMS_REPLICATION_MANAGER_STREAMS_REPLICATION_MANAGER_SERVICE_healthy_thresholds

Required

false

Other

Streams Replication Manager Cluster alias

Description

Specifies cluster aliases for the clusters SRM is connecting to. Cluster aliases are comma delimited. For example, 'primary, backup'.

Related Name

clusters

Default Value

API Name

clusters

Required

true

Streams Replication Manager Co-located Kafka Cluster Alias

Description

Alias for co-located kafka cluster. Set this only if Kafka is available on the cluster where SRM lives, and replication is needed for that Kafka cluster. For this property to have any effect, the dependency on the co-located Kafka should be activated.

Related Name

colocated.cluster.alias

Default Value

API Name

colocated.cluster.alias

Required

false

Emit Checkpoints Interval Seconds

Description

The interval at which SRM emits checkpoint information.

Related Name

emit.checkpoints.interval.seconds

Default Value

5 second(s)

API Name

emit.checkpoints.interval.seconds

Required

true

External Kafka Accounts

Description

Specifies the list of external Kafka accounts to be imported into the SRM configuration.

Related Name

external_kafka_accounts

Default Value

API Name

external_kafka_accounts

Required

false

Kafka Service

Description

Name of the Kafka service that this Streams Replication Manager service instance depends on

Related Name

Default Value

API Name

kafka_service

Required

false

Enable Kerberos Authentication

Description

Enables Kerberos authentication for this Streams Replication Manager.

Related Name

kerberos.auth.enable

Default Value

false

API Name

kerberos.auth.enable

Required

false

Replication Factor for Metrics Topics

Description

Replication factor for all metrics topics.

Related Name

metrics.topic.replication.factor

Default Value

3

API Name

metrics.topic.replication.factor

Required

false

Refresh Groups Interval Seconds

Description

The interval at which SRM looks for new consumer groups on source clusters.

Related Name

refresh.groups.interval.seconds

Default Value

10 minute(s)

API Name

refresh.groups.interval.seconds

Required

true

Refresh Topics Interval Seconds

Description

The interval at which SRM looks for new topics on source clusters.

Related Name

refresh.topics.interval.seconds

Default Value

10 minute(s)

API Name

refresh.topics.interval.seconds

Required

true

SRM_HEAP_OPTS

Description

Memory heap params.

Related Name

SRM_HEAP_OPTS

Default Value

-Xmx8G -Xms1G

API Name

SRM_HEAP_OPTS

Required

false

SRM_JMX_OPTS

Description

Change parameters to setup jmxremote.

Related Name

SRM_JMX_OPTS

Default Value

-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.management.jmxremote.ssl=false

API Name

SRM_JMX_OPTS

Required

false

SRM_JVM_PERF_OPTS

Description

SRM JVM perf and gc opts.

Related Name

SRM_JVM_PERF_OPTS

Default Value

-server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -XX:+ExplicitGCInvokesConcurrent -Djava.awt.headless=true

API Name

SRM_JVM_PERF_OPTS

Required

false

Streams Replication Manager's Replication Configs

Description

Specifies cluster bootstrap server information and cluster replication pairs.
Bootstrap information for each alias defined in the clusters property has to be added as follows: 'primary.bootstrap.servers=mycluster1.example.com:9092', 'backup.bootstrap.servers=mycluster2.example.com:9092'.. Each cluster configuration has to be added in a new line, if cluster has multiple nodes, add all nodes to the same line and delimit each with a comma. Cluster replication pairs can be defined as follows: 'primary->backup.enabled=true'.. Each unique replication pair has to be added in a new line.

Related Name

streams.replication.manager.config

Default Value

API Name

streams.replication.manager.config

Required

false

Sync Topic Acls Enabled

Description

Enables the monitoring of the source cluster for ACL changes.

Related Name

sync.topic.acls.enabled

Default Value

false

API Name

sync.topic.acls.enabled

Required

true

Sync Topic Acls Interval Seconds

Description

The interval at which SRM checks the source cluster for ACL changes.

Related Name

sync.topic.acls.interval.seconds

Default Value

30 second(s)

API Name

sync.topic.acls.interval.seconds

Required

true

Sync Topic Configs Interval Seconds

Description

The interval at which SRM checks the source cluster for configuration changes.

Related Name

sync.topic.configs.interval.seconds

Default Value

10 minute(s)

API Name

sync.topic.configs.interval.seconds

Required

true

Tasks Max

Description

Maximum number of tasks for replication between clusters.

Related Name

tasks.max

Default Value

3

API Name

tasks.max

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

streamsrepmgr

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: SRM Client's Kerberos Keytab Location

Description

Whether to suppress configuration warnings produced by the SRM Client's Kerberos Keytab Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos.keytab.location

Required

true

Suppress Configuration Validator: SRM Client's Kerberos Principal Name

Description

Whether to suppress configuration warnings produced by the SRM Client's Kerberos Principal Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos.principal.name

Required

true

Suppress Configuration Validator: SRM Driver Log Directory

Description

Whether to suppress configuration warnings produced by the SRM Driver Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: SRM Driver XML Override

Description

Whether to suppress configuration warnings produced by the SRM Driver XML Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: SRM Client's Secure Storage Password

Description

Whether to suppress configuration warnings produced by the SRM Client's Secure Storage Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.password

Required

true

Suppress Configuration Validator: Environment Variable Holding SRM Client's Secure Storage Password

Description

Whether to suppress configuration warnings produced by the Environment Variable Holding SRM Client's Secure Storage Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.password.variable

Required

true

Suppress Configuration Validator: SRM Client's Secure Storage Type

Description

Whether to suppress configuration warnings produced by the SRM Client's Secure Storage Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_securestorage.type

Required

true

Suppress Configuration Validator: SRM Service Advanced Configuration Snippet (Safety Valve) for srm-service.yaml

Description

Whether to suppress configuration warnings produced by the SRM Service Advanced Configuration Snippet (Safety Valve) for srm-service.yaml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_srm-service.yaml_role_safety_valve

Required

true

Suppress Configuration Validator: SRM Driver Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

Whether to suppress configuration warnings produced by the SRM Driver Advanced Configuration Snippet (Safety Valve) for srm.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_srm.properties_role_safety_valve

Required

true

Suppress Configuration Validator: SRM Client's TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the SRM Client's TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.keypassword

Required

true

Suppress Configuration Validator: Keystore file Location for the SRM client's TLS/SSL server

Description

Whether to suppress configuration warnings produced by the Keystore file Location for the SRM client's TLS/SSL server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.location

Required

true

Suppress Configuration Validator: SRM Client's TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the SRM Client's TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl.keystore.password

Required

true

Suppress Configuration Validator: SRM Driver TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the SRM Driver TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: SRM Driver TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the SRM Driver TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: SRM Driver TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the SRM Driver TLS/SSL Server Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: SRM Driver TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the SRM Driver TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: SRM Driver TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the SRM Driver TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Streams Replication Manager Driver Target Cluster

Description

Whether to suppress configuration warnings produced by the Streams Replication Manager Driver Target Cluster configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.driver.target.cluster

Required

true

Suppress Configuration Validator: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the Java Home Path Override configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.jdk.home

Required

true

Suppress Configuration Validator: Log Format

Description

Whether to suppress configuration warnings produced by the Log Format configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.log.format

Required

true

Suppress Configuration Validator: SRM Service Port

Description

Whether to suppress configuration warnings produced by the SRM Service Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.port

Required

true

Suppress Configuration Validator: SRM Service Https Port

Description

Whether to suppress configuration warnings produced by the SRM Service Https Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.ssl.port

Required

true

Suppress Configuration Validator: Streams Replication Manager Service Target Cluster

Description

Whether to suppress configuration warnings produced by the Streams Replication Manager Service Target Cluster configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.target.cluster

Required

true

Suppress Configuration Validator: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the SSL Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.keystoretype

Required

true

Suppress Configuration Validator: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the SSL TrustStore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.truststoretype

Required

true

Suppress Configuration Validator: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the SSL ValidateCerts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.validatecerts

Required

true

Suppress Configuration Validator: SSL ValidatePeers

Description

Whether to suppress configuration warnings produced by the SSL ValidatePeers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.validatepeers

Required

true

Suppress Configuration Validator: Streams Replication Manager Client Advanced Configuration Snippet (Safety Valve) for streams_replication_manager-conf/srm.properties

Description

Whether to suppress configuration warnings produced by the Streams Replication Manager Client Advanced Configuration Snippet (Safety Valve) for streams_replication_manager-conf/srm.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager-conf/srm.properties_client_config_safety_valve

Required

true

Suppress Configuration Validator: SRM Driver Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the SRM Driver Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager_driver_role_env_safety_valve

Required

true

Suppress Configuration Validator: SRM Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the SRM Service Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager_service_role_env_safety_valve

Required

true

Suppress Parameter Validation: Streams Replication Manager Cluster alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Cluster alias parameter.

Related Name

Default Value

false

API Name

service_config_suppression_clusters

Required

true

Suppress Parameter Validation: Streams Replication Manager Co-located Kafka Cluster Alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Co-located Kafka Cluster Alias parameter.

Related Name

Default Value

false

API Name

service_config_suppression_colocated.cluster.alias

Required

true

Suppress Parameter Validation: External Kafka Accounts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the External Kafka Accounts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_external_kafka_accounts

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Replication Factor for Metrics Topics

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Replication Factor for Metrics Topics parameter.

Related Name

Default Value

false

API Name

service_config_suppression_metrics.topic.replication.factor

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Streams Replication Manager Service Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Service Advanced Configuration Snippet (Safety Valve) for srm.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_srm.properties_service_safety_valve

Required

true

Suppress Parameter Validation: SRM_HEAP_OPTS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM_HEAP_OPTS parameter.

Related Name

Default Value

false

API Name

service_config_suppression_srm_heap_opts

Required

true

Suppress Parameter Validation: SRM_JMX_OPTS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM_JMX_OPTS parameter.

Related Name

Default Value

false

API Name

service_config_suppression_srm_jmx_opts

Required

true

Suppress Parameter Validation: SRM_JVM_PERF_OPTS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM_JVM_PERF_OPTS parameter.

Related Name

Default Value

false

API Name

service_config_suppression_srm_jvm_perf_opts

Required

true

Suppress Parameter Validation: Streams Replication Manager's Replication Configs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager's Replication Configs parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streams.replication.manager.config

Required

true

Suppress Configuration Validator: SRM Driver Count Validator

Description

Whether to suppress configuration warnings produced by the SRM Driver Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streams_replication_manager_driver_count_validator

Required

true

Suppress Configuration Validator: SRM Service Count Validator

Description

Whether to suppress configuration warnings produced by the SRM Service Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_streams_replication_manager_service_count_validator

Required

true

Suppress Parameter Validation: Streams Replication Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_streams_replication_manager_service_env_safety_valve

Required

true

Suppress Health Test: SRM Driver Health

Description

Whether to suppress the results of the SRM Driver Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_streams_replication_manager_streams_replication_manager_driver_healthy

Required

true

Suppress Health Test: SRM Service Health

Description

Whether to suppress the results of the SRM Service Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_streams_replication_manager_streams_replication_manager_service_healthy

Required

true

SRM Driver

Advanced

SRM Driver XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for SRM Driver, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from

publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

SRM Driver Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

For advanced use only. A string to be inserted into srm.properties for this role only.

Related Name

Default Value

API Name

srm.properties_role_safety_valve

Required

false

SRM Driver Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMS_REPLICATION_MANAGER_DRIVER_role_env_safety_valve

Required

false

Logs

SRM Driver Log Directory

Description

The log directory for log files of the role SRM Driver.

Related Name

log_dir

Default Value

/var/log/streams-replication-manager

API Name

log_dir

Required

false

SRM Driver Logging Threshold

Description

The minimum log level for SRM Driver logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

SRM Driver Maximum Log File Backups

Description

The maximum number of rolled log files to keep for SRM Driver logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

SRM Driver Max Log Size

Description

The maximum size, in megabytes, per log file for SRM Driver logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streams_replication_manager_driver_fd_thresholds

Required

false

SRM Driver Host Health Test

Description

When computing the overall SRM Driver health, consider the host's health.

Related Name

Default Value

true

API Name

streams_replication_manager_driver_host_health_enabled

Required

false

SRM Driver Process Health Test

Description

Enables the health test that the SRM Driver's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streams_replication_manager_driver_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Streams Replication Manager Driver Target Cluster

Description

Target cluster aliases for the srm-driver. When set, the srm-driver will collect data from all clusters, but will only write to the clusters specified here. Cluster aliases are comma separated.

Related Name

streams.replication.manager.driver.target.cluster

Default Value

API Name

streams.replication.manager.driver.target.cluster

Required

false

Java Home Path Override

Description

Java Home Path Override for Streams Replication Manager. If left empty, the java shipped with CM is used.

Related Name

streams.replication.manager.jdk.home

Default Value

API Name

streams.replication.manager.jdk.home

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

SRM Driver TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that SRM Driver might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

SRM Driver TLS/SSL Trust Store Password

Description

The password for the SRM Driver TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for SRM Driver

Description

Encrypt communication between clients and SRM Driver using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

SRM Driver TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when SRM Driver is acting as a TLS/SSL server.

Related Name

ssl.key.password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

SRM Driver TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when SRM Driver is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

SRM Driver TLS/SSL Server Keystore File Password

Description

The password for the SRM Driver keystore file.

Related Name

ssl.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: SRM Driver Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: SRM Driver XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: SRM Driver Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver Advanced Configuration Snippet (Safety Valve) for srm.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_srm.properties_role_safety_valve

Required

true

Suppress Parameter Validation: SRM Driver TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: SRM Driver TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: SRM Driver TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: SRM Driver TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: SRM Driver TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Streams Replication Manager Driver Target Cluster

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Driver Target Cluster parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.driver.target.cluster

Required

true

Suppress Parameter Validation: Java Home Path Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Home Path Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.jdk.home

Required

true

Suppress Parameter Validation: SRM Driver Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Driver Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager_driver_role_env_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_driver_unexpected_exits

Required

true

SRM Service

Advanced

SRM Service XML Override

Description

For advanced use only, replace entire XML in the logback configuration file for SRM Service, ignoring all logging configuration.

Related Name

logback_safety_valve

Default Value

API Name

logback_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

SRM Service Advanced Configuration Snippet (Safety Valve) for srm-service.yaml

Description

For advanced use only. A string to be inserted into srm-service.yaml for this role only.

Related Name

Default Value

API Name

srm-service.yaml_role_safety_valve

Required

false

SRM Service Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

For advanced use only. A string to be inserted into srm.properties for this role only.

Related Name

Default Value

API Name

srm.properties_role_safety_valve

Required

false

SRM Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STREAMS_REPLICATION_MANAGER_SERVICE_role_env_safety_valve

Required

false

Logs

SRM Service Log Directory

Description

The log directory for log files of the role SRM Service.

Related Name

log_dir

Default Value

/var/log/streams-replication-manager

API Name

log_dir

Required

false

SRM Service Logging Threshold

Description

The minimum log level for SRM Service logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

SRM Service Maximum Log File Backups

Description

The maximum number of rolled log files to keep for SRM Service logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

SRM Service Max Log Size

Description

The maximum size, in megabytes, per log file for SRM Service logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE,

$ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

streams_replication_manager_service_fd_thresholds

Required

false

SRM Service Host Health Test

Description

When computing the overall SRM Service health, consider the host's health.

Related Name

Default Value

true

API Name

streams_replication_manager_service_host_health_enabled

Required

false

SRM Service Process Health Test

Description

Enables the health test that the SRM Service's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

streams_replication_manager_service_scm_health_enabled

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Log Format

Description

Format of the messages output by logger.

Related Name

streams.replication.manager.log.format

Default Value

%dISO8601 %p %c: %m%n%rEx

API Name

streams.replication.manager.log.format

Required

false

SRM Service Port

Description

SRM Service port.

Related Name

streams.replication.manager.service.port

Default Value

6670

API Name

streams.replication.manager.service.port

Required

true

SRM Service Https Port

Description

SRM Service https port.

Related Name

streams.replication.manager.service.ssl.port

Default Value

6671

API Name

streams.replication.manager.service.ssl.port

Required

true

SRM Service Metrics Grace Period

Description

SRM Service Metrics grace period in ms. Reject out-of-order events that arrive more than millisAfterWindowEnd after the end of its window.

Related Name

streams.replication.manager.service.streams.metrics.grace

Default Value

1 minute(s)

API Name

streams.replication.manager.service.streams.metrics.grace

Required

true

SRM Service Metrics Retention Period

Description

SRM Service Metrics retention period in ms. Note that the retention period must be at least long enough to contain the windowed data's entire life cycle, from window-start through window-end, and for the entire grace period. (> 60 000 + metrics.grace)

Related Name

streams.replication.manager.service.streams.metrics.retention

Default Value

1 hour(s)

API Name

streams.replication.manager.service.streams.metrics.retention

Required

true

Streams Replication Manager Service Target Cluster

Description

Target cluster from which the SRM Service collects data.

Related Name

streams.replication.manager.service.target.cluster

Default Value

API Name

streams.replication.manager.service.target.cluster

Required

true

SSL Keystore Type

Description

The keystore type. Required if SSL is enabled for the SRM Service. For example, PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.

Related Name

streams.replication.manager.ssl.keyStoreType

Default Value

API Name

streams.replication.manager.ssl.keyStoreType

Required

false

SSL TrustStore Type

Description

The truststore type. Required if SSL is enabled for the SRM Service. For example, PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.

Related Name

streams.replication.manager.ssl.trustStoreType

Default Value

API Name

streams.replication.manager.ssl.trustStoreType

Required

false

SSL ValidateCerts

Description

Whether or not to validate TLS certificates before starting. If enabled, it will refuse to start with expired or otherwise invalid certificates. Note: if this is enabled, the certificate revocation method (CRLDP/OCSP) is also needed. This can be done by overriding Dropwizard configuration with Java system properties. E.g: -Ddw.server.applicationConnectors[0].enableCRLDP=true (more details at https://www.dropwizard.io/en/latest/manual/core.html)

Related Name

streams.replication.manager.ssl.validateCerts

Default Value

false

API Name

streams.replication.manager.ssl.validateCerts

Required

false

SSL ValidatePeers

Description

Whether or not to validate TLS peer certificates.

Related Name

streams.replication.manager.ssl.validatePeers

Default Value

false

API Name

streams.replication.manager.ssl.validatePeers

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command:

resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not

managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

SRM Service TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that SRM Service might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

SRM Service TLS/SSL Trust Store Password

Description

The password for the SRM Service TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for SRM Service

Description

Encrypt communication between clients and SRM Service using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

SRM Service TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when SRM Service is acting as a TLS/SSL server.

Related Name

ssl.key.password

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

SRM Service TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when SRM Service is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

ssl.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

SRM Service TLS/SSL Server Keystore File Password

Description

The password for the SRM Service keystore file.

Related Name

ssl.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: SRM Service Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: SRM Service XML Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service XML Override parameter.

Related Name

Default Value

false

API Name

role_config_suppression_logback_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: SRM Service Advanced Configuration Snippet (Safety Valve) for srm-service.yaml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Advanced Configuration Snippet (Safety Valve) for srm-service.yaml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_srm-service.yaml_role_safety_valve

Required

true

Suppress Parameter Validation: SRM Service Advanced Configuration Snippet (Safety Valve) for srm.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Advanced Configuration Snippet (Safety Valve) for srm.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_srm.properties_role_safety_valve

Required

true

Suppress Parameter Validation: SRM Service TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: SRM Service TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: SRM Service TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: SRM Service TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: SRM Service TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Log Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Log Format parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.log.format

Required

true

Suppress Parameter Validation: SRM Service Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.port

Required

true

Suppress Parameter Validation: SRM Service Https Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Https Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.ssl.port

Required

true

Suppress Parameter Validation: Streams Replication Manager Service Target Cluster

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Streams Replication Manager Service Target Cluster parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.service.target.cluster

Required

true

Suppress Parameter Validation: SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.keystoretype

Required

true

Suppress Parameter Validation: SSL TrustStore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL TrustStore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.truststoretype

Required

true

Suppress Parameter Validation: SSL ValidateCerts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL ValidateCerts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.validatecerts

Required

true

Suppress Parameter Validation: SSL ValidatePeers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SSL ValidatePeers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams.replication.manager.ssl.validatepeers

Required

true

Suppress Parameter Validation: SRM Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SRM Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_streams_replication_manager_service_role_env_safety_valve

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_streams_replication_manager_streams_replication_manager_service_unexpected_exits

Required

true

Stub DFS Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hadoop

API Name

client_config_root_dir

Required

true

Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hadoop-env.sh

Related Name

Default Value

API Name

core_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

core_client_java_opts

Required

false

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

core_client_java_heapsize

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_java_opts

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as (except the HttpFS server, which has its own group)

Related Name

Default Value

hdfs

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

hdfs

API Name

process_username

Required

true

Stub DFS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

STUB_DFS_service_env_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Core Settings Connector

Description

Dependency on the Core Settings service for the cluster.

Related Name

Default Value

API Name

core_connector

Required

true

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

hdfs

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_java_opts

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Gateway Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Storage Operations Log Directory

Description

Whether to suppress configuration warnings produced by the Storage Operations Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_storageoperations_log_dir

Required

true

Suppress Configuration Validator: Storage Operations Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Storage Operations Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_storageoperations_role_env_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Configuration Validator: Stub DFS only DFS Validator

Description

Whether to suppress configuration warnings produced by the Stub DFS only DFS Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_only_dfs_in_cluster_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Storage Operations Count Validator

Description

Whether to suppress configuration warnings produced by the Storage Operations Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_storageoperations_count_validator

Required

true

Suppress Parameter Validation: Stub DFS Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stub DFS Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_stub_dfs_service_env_safety_valve

Required

true

Storage Operations

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hadoop

API Name

client_config_root_dir

Required

true

Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hadoop-env.sh

Related Name

Default Value

API Name

core_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

core_client_java_opts

Required

false

Storage Operations Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Storage Operations Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

STORAGEOPERATIONS_role_env_safety_valve

Required

false

Logs

Storage Operations Logging Threshold

Description

The minimum log level for Storage Operations logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Storage Operations Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Storage Operations logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Storage Operations Max Log Size

Description

The maximum size, in megabytes, per log file for Storage Operations logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Storage Operations Log Directory

Description

Directory where Storage Operations will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/

API Name

storageoperations_log_dir

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

90

API Name

client_config_priority

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

core_client_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Core Configuration Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_core_client_java_opts

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Storage Operations Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Operations Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Storage Operations Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Operations Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_storageoperations_log_dir

Required

true

Suppress Parameter Validation: Storage Operations Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Storage Operations Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_storageoperations_role_env_safety_valve

Required

true

Tez Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/tez

API Name

client_config_root_dir

Required

true

Tez Client Advanced Configuration Snippet (Safety Valve) for tez-conf/tez-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for tez-conf/tez-site.xml.

Related Name

Default Value

API Name

tez-conf/tez-site.xml_client_config_safety_valve

Required

false

Monitoring

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

50

API Name

client_config_priority

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Tez Client Advanced Configuration Snippet (Safety Valve) for tez-conf/tez-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Client Advanced Configuration Snippet (Safety Valve) for tez-conf/tez-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_tez-conf/tez-site.xml_client_config_safety_valve

Required

true

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hadoop

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

tez

API Name

process_username

Required

true

Tez Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

TEZ_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Maximum Heartbeat Interval

Description

The maximum heartbeat interval between the Application Master and RM in milliseconds.

Related Name

tez.am.am-rm.heartbeat.interval-ms.max

Default Value

250 millisecond(s)

API Name

tez.am.am-rm.heartbeat.interval-ms.max

Required

true

Maximum Timeout to Hold Idle Containers

Description

The maximum amount of time to hold on to a container if no task can be assigned to it immediately. Only active when reuse is enabled.

Related Name

tez.am.container.idle.release-timeout-max.millis

Default Value

20 second(s)

API Name

tez.am.container.idle.release-timeout-max.millis

Required

true

Minimum Timeout to Hold Idle Containers

Description

The minimum amount of time to hold on to a container that is idle. Only active when reuse is enabled.

Related Name

tez.am.container.idle.release-timeout-min.millis

Default Value

10 second(s)

API Name

tez.am.container.idle.release-timeout-min.millis

Required

true

Enable Container Reuse

Description

Configuration to specify whether container should be reused.

Related Name

tez.am.container.reuse.enabled

Default Value

true

API Name

tez.am.container.reuse.enabled

Required

true

Timeout Before Container Reuse

Description

The amount of time to wait before assigning a container to the next level of locality. NODE > RACK > NON_LOCAL

Related Name

tez.am.container.reuse.locality.delay-allocation-millis

Default Value

250 millisecond(s)

API Name

tez.am.container.reuse.locality.delay-allocation-millis

Required

true

Enable Container Reuse for Non-Local Tasks

Description

Whether to reuse containers for non-local tasks. Active only if reuse is enabled.

Related Name

tez.am.container.reuse.non-local-fallback.enabled

Default Value

false

API Name

tez.am.container.reuse.non-local-fallback.enabled

Required

true

Enable Container Reuse for Rack Local Tasks

Description

Whether to reuse containers for rack local tasks. Active only if reuse is enabled.

Related Name

tez.am.container.reuse.rack-fallback.enabled

Default Value

true

API Name

tez.am.container.reuse.rack-fallback.enabled

Required

true

Tez Application Master Command Line Options

Description

Java options for the Tez Application Master process. The Xmx value is derived based on tez.am.resource.memory.mb and is 80% of the value by default. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.am.launch.cmd-opts

Default Value

-XX:+PrintGCDetails -verbose:gc -XX:+UseNUMA -XX:+UseG1GC -XX:+ResizeTLAB -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/tmp -XX:+IgnoreUnrecognizedVMOptions --add-opens=java.base/java.net=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent.atomic=ALL-UNNAMED --add-opens=java.base/java.util.regex=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.time=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED

API Name

tez.am.launch.cmd-opts

Required

true

Tez Application Master Environment Settings

Description

Additional execution environment entries for tez. This is not an additive property. You must preserve the original value if you want to have access to native libraries. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.am.launch.env

Default Value

LD_LIBRARY_PATH=$PARCELS_ROOT/CDH/lib/hadoop/lib/native

API Name

tez.am.launch.env

Required

true

Log level for Application Masters

Description

Root Logging level passed to the Tez Application Master.

Related Name

tez.am.log.level

Default Value

INFO

API Name

tez.am.log.level

Required

true

Number of Recovery Runs

Description

Specifies the total number of time the Application Master will run in case recovery is triggered.

Related Name

tez.am.max.app.attempts

Default Value

2

API Name

tez.am.max.app.attempts

Required

true

Maximum Task Attempts

Description

The maximum number of allowed task attempt failures on a node before it gets marked as blacklisted.

Related Name

tez.am.maxtaskfailures.per.node

Default Value

10

API Name

tez.am.maxtaskfailures.per.node

Required

true

Tez Application Master Memory

Description

The amount of memory to be used by the Application Master. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.am.resource.memory.mb

Default Value

2 GiB

API Name

tez.am.resource.memory.mb

Required

true

History URL Template

Description

Template to generate the History URL for a particular Tez Application. Template replaces __APPLICATION_ID__ with the actual applicationId and __HISTORY_URL_BASE__ with the value from the tez.tez-ui.history-url.base config property

Related Name

tez.am.tez-ui.history-url.template

Default Value

__HISTORY_URL_BASE__?viewPath=%2F%23%2Ftez-app%2F__APPLICATION_ID__

API Name

tez.am.tez-ui.history-url.template

Required

true

Tez Application Master View ACLs

Description

Application Master view ACLs. This allows the specified users/groups to view the status of the Application Master and all DAGs that run within this Appliation Master. Value format: Comma separated list of users, followed by whitespace, followed by a comma separated list of groups.

Related Name

tez.am.view-acls

Default Value

*

API Name

tez.am.view-acls

Required

false

Tez Additional Classpath

Description

Specify additional classpath information to be used for Tez AM and all containers.

Related Name

tez.cluster.additional.classpath.prefix

Default Value

API Name

tez.cluster.additional.classpath.prefix

Required

false

Maximum Number of Counters

Description

The number of allowed counters for the executing DAG.

Related Name

tez.counters.max

Default Value

10000

API Name

tez.counters.max

Required

true

Maximum Counter Groups

Description

The number of allowed counter groups for the executing DAG.

Related Name

tez.counters.max.groups

Default Value

3000

API Name

tez.counters.max.groups

Required

true

Whether to generate debug artifacts

Description

Generate debug artifacts such as a text representation of the submitted DAG plan.

Related Name

tez.generate.debug.artifacts

Default Value

false

API Name

tez.generate.debug.artifacts

Required

true

Grouped Split Maximum Size

Description

Upper bound on the size (in bytes) of a grouped split, to avoid generating excessively large split.

Related Name

tez.grouping.max-size

Default Value

1 GiB

API Name

tez.grouping.max-size

Required

true

Grouped Split Minimum Size

Description

Lower bound on the size (in bytes) of a grouped split, to avoid generating too many splits.

Related Name

tez.grouping.min-size

Default Value

16 MiB

API Name

tez.grouping.min-size

Required

true

Queue Capacity Multiplier

Description

The multiplier for available queue capacity when determining number of tasks for a Vertex. 1.7 with 100% queue available implies generating a number of tasks roughly equal to 170% of the available containers on the queue.

Related Name

tez.grouping.split-waves

Default Value

1.7

API Name

tez.grouping.split-waves

Required

true

Tez history events directory

Description

Directory where proto logger writes the history events, should generally be sys.db database directory.

Related Name

tez.history.logging.proto-base-dir

Default Value

/warehouse/tablespace/managed/hive/sys.db

API Name

tez.history.logging.proto-base-dir

Required

true

DAGs per Group

Description

DAGs per group.

Related Name

tez.history.logging.timeline-cache-plugin.old-num-dags-per-group

Default Value

5

API Name

tez.history.logging.timeline-cache-plugin.old-num-dags-per-group

Required

true

Enable Intermediate Data Compression

Description

Whether intermediate data should be compressed or not.

Related Name

tez.runtime.compress

Default Value

true

API Name

tez.runtime.compress

Required

true

Codec for Compressing Intermediate Data

Description

The codec to be used if compressing intermediate data. Only applicable if tez.runtime.compress is enabled.

Related Name

tez.runtime.compress.codec

Default Value

org.apache.hadoop.io.compress.SnappyCodec

API Name

tez.runtime.compress.codec

Required

true

Publish Configuration Information

Description

Whether to publish configuration information to History logger.

Related Name

tez.runtime.convert.user-payload.to.history-text

Default Value

false

API Name

tez.runtime.convert.user-payload.to.history-text

Required

true

Sort Buffer Size

Description

The size of the sort buffer when output needs to be sorted.

Related Name

tez.runtime.io.sort.mb

Default Value

272 MiB

API Name

tez.runtime.io.sort.mb

Required

true

Enable Accessing the Local Files Directly

Description

If the shuffle input is on the local host bypass the http fetch and access the files directly.

Related Name

tez.runtime.optimize.local.fetch

Default Value

true

API Name

tez.runtime.optimize.local.fetch

Required

true

Pipeline Sorter Sort Threads

Description

Tez runtime pipelined sorter sort threads.

Related Name

tez.runtime.pipelined.sorter.sort.threads

Default Value

2

API Name

tez.runtime.pipelined.sorter.sort.threads

Required

true

Fraction of Memory to Retain Shuffled Data

Description

Fraction (0-1) of the available memory which can be used to retain shuffled data.

Related Name

tez.runtime.shuffle.fetch.buffer.percent

Default Value

0.6

API Name

tez.runtime.shuffle.fetch.buffer.percent

Required

true

Keep the Shuffle Connection Alive

Description

This property determines if the shuffle connection should be kept alive. If not, then the connection needs to be reestablished.

Related Name

tez.runtime.shuffle.keep-alive.enabled

Default Value

true

API Name

tez.runtime.shuffle.keep-alive.enabled

Required

true

Maximum Percent of Shuffle Segment

Description

This property determines the maximum size of a shuffle segment which can be fetched to memory. Fraction (0-1) of shuffle memory (after applying tez.runtime.shuffle.fetch.buffer.percent).

Related Name

tez.runtime.shuffle.memory.limit.percent

Default Value

0.25

API Name

tez.runtime.shuffle.memory.limit.percent

Required

true

Buffer Size for Unordered Output

Description

The size of the buffer when output does not require to be sorted.

Related Name

tez.runtime.unordered.output.buffer.size-mb

Default Value

100 MiB

API Name

tez.runtime.unordered.output.buffer.size-mb

Required

true

Timeout for Application Master for a Task

Description

Time (in seconds) for which the Tez Application Master should wait for a DAG to be submitted before shutting down.

Related Name

tez.session.am.dag.submit.timeout.secs

Default Value

5 minute(s)

API Name

tez.session.am.dag.submit.timeout.secs

Required

true

Timeout for Application Master to Come up

Description

Time (in seconds) to wait for Application Master to come up when trying to submit a DAG from the client.

Related Name

tez.session.client.timeout.secs

Default Value

-1 second(s)

API Name

tez.session.client.timeout.secs

Required

true

ScatterGather Connection Maximum Fraction of Tasks

Description

In case of a ScatterGather connection, once this fraction of source tasks have completed, all tasks on the current vertex can be scheduled. Number of tasks ready for scheduling on the current vertex scales linearly between min-fraction and max-fraction.

Related Name

tez.shuffle-vertex-manager.max-src-fraction

Default Value

0.4

API Name

tez.shuffle-vertex-manager.max-src-fraction

Required

true

ScatterGather Connection Minimum Fraction of Tasks

Description

In case of a ScatterGather connection, the fraction of source tasks which should complete before tasks for the current vertex are schedule.

Related Name

tez.shuffle-vertex-manager.min-src-fraction

Default Value

0.2

API Name

tez.shuffle-vertex-manager.min-src-fraction

Required

true

TEZ Staging directory

Description

The staging dir used while submitting DAGs.

Related Name

tez.staging-dir

Default Value

/tmp/$user.name/staging

API Name

tez.staging-dir

Required

true

Heartbeat Interval

Description

Time interval at which task counters are sent to the Application Master.

Related Name

tez.task.am.heartbeat.counter.interval-ms.max

Default Value

4 second(s)

API Name

tez.task.am.heartbeat.counter.interval-ms.max

Required

true

Generate Counters on a Per-Edge Basis

Description

Whether to generate counters on a per-edge basis for a Tez DAG. Helpful for in-depth analysis.

Related Name

tez.task.generate.counters.per.io

Default Value

true

API Name

tez.task.generate.counters.per.io

Required

true

Maximum Time Between Tasks

Description

The maximum amount of time, in seconds, to wait before a task asks an Application Master for another task.

Related Name

tez.task.get-task.sleep.interval-ms.max

Default Value

200 millisecond(s)

API Name

tez.task.get-task.sleep.interval-ms.max

Required

true

Tez Task Command Line Options

Description

Java options for tasks. The Xmx value is derived based on tez.task.resource.memory.mb and is 80% of this value by default. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.task.launch.cmd-opts

Default Value

-XX:+PrintGCDetails -verbose:gc -XX:+UseNUMA -XX:+UseG1GC -XX:+ResizeTLAB -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/tmp -XX:+IgnoreUnrecognizedVMOptions --add-opens=java.base/java.net=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent.atomic=ALL-UNNAMED --add-opens=java.base/java.util.regex=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.time=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED

API Name

tez.task.launch.cmd-opts

Required

true

Tez Task Environment Settings

Description

Additional execution environment entries for tez. This is not an additive property. You must preserve the original value if you want to have access to native libraries. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.task.launch.env

Default Value

LD_LIBRARY_PATH=$PARCELS_ROOT/CDH/lib/hadoop/lib/native

API Name

tez.task.launch.env

Required

true

Maximum Number of Events in a Heartbeat

Description

Maximum number of events to fetch from the Application Master by the tasks in a single heartbeat.

Related Name

tez.task.max-events-per-heartbeat

Default Value

500

API Name

tez.task.max-events-per-heartbeat

Required

true

Tez Task Memory

Description

The amount of memory to be used by launched tasks. Used only if the value is not specified explicitly by the DAG definition.

Related Name

tez.task.resource.memory.mb

Default Value

1536 MiB

API Name

tez.task.resource.memory.mb

Required

true

Tez UI URL Base

Description

The base of the Tez UI URL.

Related Name

tez.tez-ui.history-url.base

Default Value

API Name

tez.tez-ui.history-url.base

Required

false

Use Hadoop Libs

Description

This being true implies that the deployment is relying on hadoop jars being available on the cluster on all nodes.

Related Name

tez.use.cluster.hadoop-libs

Default Value

false

API Name

tez.use.cluster.hadoop-libs

Required

true

Enable Yarn Timeline-Service

Description

Timeline service version we're currently using.

Related Name

yarn.timeline-service.enabled

Default Value

false

API Name

yarn.timeline-service.enabled

Required

true

YARN Service

Description

Name of the YARN service that this Tez service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Tez Client Advanced Configuration Snippet (Safety Valve) for tez-conf/tez-site.xml

Description

Whether to suppress configuration warnings produced by the Tez Client Advanced Configuration Snippet (Safety Valve) for tez-conf/tez-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_tez-conf/tez-site.xml_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: Tez Application Master Command Line Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Application Master Command Line Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.am.launch.cmd-opts

Required

true

Suppress Parameter Validation: Tez Application Master Environment Settings

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Application Master Environment Settings parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.am.launch.env

Required

true

Suppress Parameter Validation: Number of Recovery Runs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Number of Recovery Runs parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.am.max.app.attempts

Required

true

Suppress Parameter Validation: History URL Template

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the History URL Template parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.am.tez-ui.history-url.template

Required

true

Suppress Parameter Validation: Tez Application Master View ACLs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Application Master View ACLs parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.am.view-acls

Required

true

Suppress Parameter Validation: Tez Additional Classpath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Additional Classpath parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.cluster.additional.classpath.prefix

Required

true

Suppress Parameter Validation: Tez history events directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez history events directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.history.logging.proto-base-dir

Required

true

Suppress Parameter Validation: DAGs per Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the DAGs per Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.history.logging.timeline-cache-plugin.old-num-dags-per-group

Required

true

Suppress Parameter Validation: Codec for Compressing Intermediate Data

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Codec for Compressing Intermediate Data parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.runtime.compress.codec

Required

true

Suppress Parameter Validation: TEZ Staging directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TEZ Staging directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.staging-dir

Required

true

Suppress Parameter Validation: Tez Task Command Line Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Task Command Line Options parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.task.launch.cmd-opts

Required

true

Suppress Parameter Validation: Tez Task Environment Settings

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Task Environment Settings parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.task.launch.env

Required

true

Suppress Parameter Validation: Tez UI URL Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez UI URL Base parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez.tez-ui.history-url.base

Required

true

Suppress Parameter Validation: Tez Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Tez Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_tez_service_env_safety_valve

Required

true

YARN Properties in Cloudera Runtime 7.2.18

Role groups:

Gateway

Advanced

Deploy Directory

Description

The directory where the client configs will be deployed

Related Name

Default Value

/etc/hadoop

API Name

client_config_root_dir

Required

true

Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

MapReduce Client Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for mapred-site.xml.

Related Name

Default Value

API Name

mapreduce_client_config_safety_valve

Required

false

Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

For advanced use only, key-value pairs (one on each line) to be inserted into the client configuration for hadoop-env.sh

Related Name

Default Value

API Name

mapreduce_client_env_safety_valve

Required

false

Client Java Configuration Options

Description

These are Java command-line arguments. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here.

Related Name

Default Value

-Djava.net.preferIPv4Stack=true

API Name

mapreduce_client_java_opts

Required

false

YARN Client Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only, a string to be inserted into the client configuration for yarn-site.xml.

Related Name

Default Value

API Name

yarn_client_config_safety_valve

Required

false

Compression

Compression Level of Codecs

Description

Compression level for the codec used to compress MapReduce outputs. Default compression is a balance between speed and compression ratio.

Related Name

zlib.compress.level

Default Value

DEFAULT_COMPRESSION

API Name

zlib_compress_level

Required

false

Logs

Gateway Logging Threshold

Description

The minimum log level for Gateway logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Monitoring

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Other

Alternatives Priority

Description

The priority level that the client configuration will have in the Alternatives system on the hosts. Higher priority levels will cause Alternatives to prefer this configuration over any others.

Related Name

Default Value

92

API Name

client_config_priority

Required

true

Client Failover Sleep Base Time

Description

Base sleep time between failover attempts. Used only if RM HA is enabled.

Related Name

yarn.client.failover-sleep-base-ms

Default Value

100 millisecond(s)

API Name

client_failover_sleep_base

Required

false

Client Failover Sleep Max Time

Description

Maximum sleep time between failover attempts. Used only if RM HA is enabled.

Related Name

yarn.client.failover-sleep-max-ms

Default Value

2 second(s)

API Name

client_failover_sleep_max

Required

false

Running Job History Location

Description

Location to store the job history files of running jobs. This is a path on the host where the JobTracker is running.

Related Name

hadoop.job.history.location

Default Value

/var/log/hadoop-mapreduce/history

API Name

hadoop_job_history_dir

Required

false

SequenceFile I/O Buffer Size

Description

Size of buffer for read and write operations of SequenceFiles.

Related Name

io.file.buffer.size

Default Value

64 KiB

API Name

io_file_buffer_size

Required

false

I/O Sort Factor

Description

The number of streams to merge at the same time while sorting files. That is, the number of sort heads to use during the merge sort on the reducer side. This determines the number of open file handles. Merging more files in parallel reduces merge sort iterations and improves run time by eliminating disk I/O. Note that merging more files in parallel uses more memory. If 'io.sort.factor' is set too high or the maximum JVM heap is set too low, excessive garbage collection will occur. The Hadoop default is 10, but Cloudera recommends a higher value. Will be part of generated client configuration.

Related Name

mapreduce.task.io.sort.factor

Default Value

64

API Name

io_sort_factor

Required

false

I/O Sort Memory Buffer (MiB)

Description

The total amount of memory buffer, in megabytes, to use while sorting files. Note that this memory comes out of the user JVM heap size (meaning total user JVM heap - this amount of memory = total user usable heap space. Note that Cloudera's default differs from Hadoop's default; Cloudera uses a bigger buffer by default because modern machines often have more RAM. The smallest value across all TaskTrackers will be part of generated client configuration.

Related Name

mapreduce.task.io.sort.mb

Default Value

256 MiB

API Name

io_sort_mb

Required

false

I/O Sort Spill Percent

Description

The soft limit in either the buffer or record collection buffers. When this limit is reached, a thread will begin to spill the contents to disk in the background. Note that this does not imply any chunking of data to the spill. A value less than 0.5 is not recommended. The syntax is in decimal units; the default is 80% and is formatted 0.8. Will be part of generated client configuration.

Related Name

mapreduce.map.sort.spill.percent

Default Value

0.8

API Name

io_sort_spill_percent

Required

false

Use Compression on Map Outputs

Description

If enabled, uses compression on the map outputs before they are sent across the network. Will be part of generated client configuration.

Related Name

mapreduce.map.output.compress

Default Value

true

API Name

mapred_compress_map_output

Required

false

Compression Codec of MapReduce Map Output

Description

For MapReduce map outputs that are compressed, specify the compression codec to use. Will be part of generated client configuration.

Related Name

mapreduce.map.output.compress.codec

Default Value

org.apache.hadoop.io.compress.SnappyCodec

API Name

mapred_map_output_compression_codec

Required

false

Map Tasks Speculative Execution

Description

If enabled, multiple instances of some map tasks may be executed in parallel.

Related Name

mapreduce.map.speculative

Default Value

false

API Name

mapred_map_tasks_speculative_execution

Required

false

Compress MapReduce Job Output

Description

Compress the output of MapReduce jobs. Will be part of generated client configuration.

Related Name

mapreduce.output.fileoutputformat.compress

Default Value

false

API Name

mapred_output_compress

Required

false

Compression Codec of MapReduce Job Output

Description

For MapReduce job outputs that are compressed, specify the compression codec to use. Will be part of generated client configuration.

Related Name

mapreduce.output.fileoutputformat.compress.codec

Default Value

org.apache.hadoop.io.compress.DefaultCodec

API Name

mapred_output_compression_codec

Required

false

Compression Type of MapReduce Job Output

Description

For MapReduce job outputs that are compressed as SequenceFiles, you can select one of these compression type options: NONE, RECORD or BLOCK. Cloudera recommends BLOCK. Will be part of generated client configuration.

Related Name

mapreduce.output.fileoutputformat.compress.type

Default Value

BLOCK

API Name

mapred_output_compression_type

Required

false

Default Number of Parallel Transfers During Shuffle

Description

The default number of parallel transfers run by reduce during the copy (shuffle) phase. This number is calculated by the following formula: min(number_of_nodes, n * min(number_of_cores_per_node, number_of_spindles_per_node)) where the n represents how many streams you want to run per core/spindle. A value of 10 for n is appropriate in most cases. Will be part of generated client configuration.

Related Name

mapreduce.reduce.shuffle.parallelcopies

Default Value

10

API Name

mapred_reduce_parallel_copies

Required

false

Number of Map Tasks to Complete Before Reduce Tasks

Description

Fraction of the number of map tasks in the job which should be completed before reduce tasks are scheduled for the job.

Related Name

mapreduce.job.reduce.slowstart.completedmaps

Default Value

0.8

API Name

mapred_reduce_slowstart_completed_maps

Required

false

Default Number of Reduce Tasks per Job

Description

The default number of reduce tasks per job. Will be part of generated client configuration.

Related Name

mapreduce.job.reduces

Default Value

1

API Name

mapred_reduce_tasks

Required

false

Reduce Tasks Speculative Execution

Description

If enabled, multiple instances of some reduce tasks may be executed in parallel.

Related Name

mapreduce.reduce.speculative

Default Value

false

API Name

mapred_reduce_tasks_speculative_execution

Required

false

Mapreduce Submit Replication

Description

The replication level for submitted job files.

Related Name

mapreduce.client.submit.file.replication

Default Value

10

API Name

mapred_submit_replication

Required

false

Mapreduce Task Timeout

Description

The number of milliseconds before a task will be terminated if it neither reads an input, writes an output, nor updates its status string.

Related Name

mapreduce.task.timeout

Default Value

10 minute(s)

API Name

mapred_task_timeout

Required

false

MR Application Environment

Description

Additional execution environment entries for map and reduce task processes.

Related Name

mapreduce.admin.user.env

Default Value

LD_LIBRARY_PATH=$HADOOP_COMMON_HOME/lib/native:$JAVA_LIBRARY_PATH

API Name

mapreduce_admin_user_env

Required

false

Maximum Number of Attempts for MapReduce Jobs

Description

The maximum number of application attempts for MapReduce jobs. The value of this parameter overrides ApplicationMaster Maximum Attempts for MapReduce jobs.

Related Name

mapreduce.am.max-attempts

Default Value

2

API Name

mapreduce_am_max_attempts

Required

false

MR Application Classpath

Description

Classpaths to include for MapReduce applications. During evaluation, the string '{version}' in the value of this parameter will be replaced by the actual MapReduce version.

Related Name

mapreduce.application.classpath

Default Value

$HADOOP_CLIENT_CONF_DIR $PWD/mr-framework/* $MR2_CLASSPATH

API Name

mapreduce_application_classpath

Required

false

MR Application Framework Path

Description

Path for MapReduce application framework. During evaluation, the string '{version}' in the value of this parameter will be replaced by the actual MapReduce version.

Related Name

mapreduce.application.framework.path

Default Value

/user/yarn/mapreduce/mr-framework/version-mr-framework.tar.gz#mr-framework

API Name

mapreduce_application_framework_path

Required

false

Application Framework

Description

The application framework to run jobs with. If not set, jobs will be run with the local job runner.

Related Name

mapreduce.framework.name

Default Value

yarn

API Name

mapreduce_framework_name

Required

false

ACL For Modifying A Job

Description

Specifies a list of users and/or groups that are allowed to modify job operations. For specifying a list of users and groups the format to use is "user1,user2 group1,group". If set to '*', it allows all users/groups to modify this job. If set to ' '(i.e. space), it allows none. Irrespective of this ACL configuration, (a) job-owner, (b) the user who started the cluster, (c) members of an admin configured supergroup configured via mapreduce.cluster.permissions.supergroup and (d) queue administrators of the queue to which this job was submitted to configured via acl-administer-jobs for the specific queue in mapred-queues.xml can do all the modification operations on a job. Ignored unless mapreduce.clouster.acls.enabled is true.

Related Name

mapreduce.job.acl-modify-job

Default Value

API Name

mapreduce_job_acl_modify_job

Required

false

ACL For Viewing A Job

Description

Specifies a list of users and/or groups that are allowed to view private job details. For specifying a list of users and groups the format to use is "user1,user2 group1,group". If set to '*', it allows all users/groups to modify this job. If set to ' '(i.e. space), it allows none. Irrespective of this ACL configuration, (a) job-owner, (b) the user who started the cluster, (c) members of an admin configured supergroup configured via mapreduce.cluster.permissions.supergroup and (d) queue administrators of the queue to which this job was submitted to configured via acl-administer-jobs for the specific queue in mapred-queues.xml can do all the view operations on a job. Ignored unless mapreduce.cluster.acls.enabled is true.

Related Name

mapreduce.job.acl-view-job

Default Value

API Name

mapreduce_job_acl_view_job

Required

false

Redacted MapReduce Job Properties

Description

A comma-separated list of job properties to redact in MapReduce.

Related Name

mapreduce.job.redacted-properties

Default Value

fs.s3a.access.key fs.s3a.secret.key fs.adl.oauth2.credential dfs.adls.oauth2.credential fs.azure.account.oauth2.client.secret

API Name

mapreduce_job_redacted_properties

Required

false

JobTracker MetaInfo Maxsize

Description

The maximum permissible size of the split metainfo file. The JobTracker won't attempt to read split metainfo files bigger than the configured value. No limits if set to -1.

Related Name

mapreduce.job.split.metainfo.maxsize

Default Value

10000000

API Name

mapreduce_jobtracker_split_metainfo_maxsize

Required

false

Map Task Java Opts Base

Description

Java opts for the map processes. The following symbol, if present, will be interpolated: @taskid@ is replaced by current TaskID. Any other occurrences of '@' will go unchanged. For example, to enable verbose gc logging to a file named for the taskid in /tmp pass a value of: "-verbose:gc -

Xloggc:/tmp/@taskid@.gc". The configuration variable 'Map Task Memory' can be used to control the maximum memory of the map processes.

Related Name

mapreduce.map.java.opts

Default Value

-Djava.net.preferIPv4Stack=true

API Name

mapreduce_map_java_opts

Required

false

Reduce Task Java Opts Base

Description

Java opts for the reduce processes. The following symbol, if present, will be interpolated: @taskid@ is replaced by current TaskID. Any other occurrences of '@' will go unchanged. For example, to enable verbose gc logging to a file named for the taskid in /tmp pass a value of: "-verbose:gc -Xloggc:/tmp/@taskid@.gc". The configuration variable 'Reduce Task Memory' can be used to control the maximum memory of the reduce processes.

Related Name

mapreduce.reduce.java.opts

Default Value

-Djava.net.preferIPv4Stack=true

API Name

mapreduce_reduce_java_opts

Required

false

ApplicationMaster Environment

Description

Environment variables for the MapReduce ApplicationMaster. These settings can be overridden in the ApplicationMaster User Environment (yarn.app.mapreduce.am.env).

Related Name

yarn.app.mapreduce.am.admin.user.env

Default Value

LD_LIBRARY_PATH=$HADOOP_COMMON_HOME/lib/native:$JAVA_LIBRARY_PATH

API Name

yarn_app_mapreduce_am_admin_user_env

Required

false

ApplicationMaster Java Opts Base

Description

Java command line arguments passed to the MapReduce ApplicationMaster.

Related Name

yarn.app.mapreduce.am.command-opts

Default Value

-Djava.net.preferIPv4Stack=true

API Name

yarn_app_mapreduce_am_command_opts

Required

false

Performance

JHist File Format

Description

File format the AM will use when generating the .jhist file. Valid values are "json" for text output and "binary" for faster parsing.

Related Name

mapreduce.jobhistory.jhist.format

Default Value

binary

API Name

mapred_jobhistory_jhist_format

Required

false

Enable Optimized Map-side Output Collector

Description

Whether map tasks should attempt to use the optimized native implementation of the map-side output collector. This can improve performance of many jobs that are shuffle-intensive. Experimental in CDH 5.2.

Related Name

Default Value

false

API Name

mapreduce_enable_native_map_output_collector

Required

false

Job Counter Groups Limit

Description

Limit on the number of counter groups allowed per job.

Related Name

mapreduce.job.counters.groups.max

Default Value

50

API Name

mapreduce_job_counter_groups_limit

Required

false

Job Counters Limit

Description

Limit on the number of counters allowed per job.

Related Name

mapreduce.job.counters.max

Default Value

120

API Name

mapreduce_job_counters_limit

Required

false

Enable Ubertask Optimization

Description

Whether to enable ubertask optimization, which runs "sufficiently small" jobs sequentially within a single JVM. "Small" is defined by the mapreduce.job.ubertask.maxmaps, mapreduce.job.ubertask.maxreduces, and mapreduce.job.ubertask.maxbytes settings.

Related Name

mapreduce.job.ubertask.enable

Default Value

false

API Name

mapreduce_job_ubertask_enabled

Required

false

Ubertask Maximum Job Size

Description

Threshold for number of input bytes, beyond which a job is considered too big for ubertask optimization. If no value is specified, dfs.block.size is used as a default.

Related Name

mapreduce.job.ubertask.maxbytes

Default Value

API Name

mapreduce_job_ubertask_maxbytes

Required

false

Ubertask Maximum Maps

Description

Threshold for number of maps, beyond which a job is considered too big for ubertask optimization.

Related Name

mapreduce.job.ubertask.maxmaps

Default Value

9

API Name

mapreduce_job_ubertask_maxmaps

Required

false

Ubertask Maximum Reduces

Description

Threshold for number of reduces, beyond which a job is considered too big for ubertask optimization. Note: As of CDH 5, MR2 does not support more than one reduce in an ubertask. (Zero is valid.)

Related Name

mapreduce.job.ubertask.maxreduces

Default Value

1

API Name

mapreduce_job_ubertask_maxreduces

Required

false

Resource Management

Client Java Heap Size in Bytes

Description

Maximum size in bytes for the Java process heap memory. Passed to Java -Xmx.

Related Name

Default Value

825955249 B

API Name

mapreduce_client_java_heapsize

Required

false

Heap to Container Size Ratio

Description

The ratio of heap size to container size for both map and reduce tasks. The heap should be smaller than the container size to allow for some overhead of the JVM.

Related Name

mapreduce.job.heap.memory-mb.ratio

Default Value

0.8

API Name

mapreduce_job_heap_memory_mb_ratio

Required

false

Map Task CPU Virtual Cores

Description

The number of virtual CPU cores allocated for each map task of a job. This parameter has no effect prior to CDH 4.4.

Related Name

mapreduce.map.cpu.vcores

Default Value

1

API Name

mapreduce_map_cpu_vcores

Required

false

Map Task Maximum Heap Size

Description

The maximum Java heap size, in bytes, of the map processes. This number will be formatted and concatenated with 'Map Task Java Opts Base' to pass to Hadoop.

Related Name

Default Value

0 B

API Name

mapreduce_map_java_opts_max_heap

Required

false

Map Task Memory

Description

The amount of physical memory, in MiB, allocated for each map task of a job. For versions before CDH 5.5, if not specified, by default it is set to 1024. For CDH 5.5 and higher, a value less than 128 is not supported but if it is specified as 0, the amount of physical memory to request is inferred from Map Task Maximum Heap Size and Heap to Container Size Ratio. If Map Task Maximum Heap Size is not specified, by default the amount of physical memory to request is set to 1024.

Related Name

mapreduce.map.memory.mb

Default Value

0 B

API Name

mapreduce_map_memory_mb

Required

false

Reduce Task CPU Virtual Cores

Description

The number of virtual CPU cores for each reduce task of a job.

Related Name

mapreduce.reduce.cpu.vcores

Default Value

1

API Name

mapreduce_reduce_cpu_vcores

Required

false

Reduce Task Maximum Heap Size

Description

The maximum Java heap size, in bytes, of the reduce processes. This number will be formatted and concatenated with 'Reduce Task Java Opts Base' to pass to Hadoop.

Related Name

Default Value

0 B

API Name

mapreduce_reduce_java_opts_max_heap

Required

false

Reduce Task Memory

Description

The amount of physical memory, in MiB, allocated for each reduce task of a job. For versions before CDH 5.5, if not specified, by default it is set to 1024. For CDH 5.5 and higher, a value less than 128 is not supported but if it is specified as 0, the amount of physical memory to request is inferred from Reduce Task Maximum Heap Size and Heap to Container Size Ratio. If Reduce Task Maximum Heap Size is not specified, by default the amount of physical memory to request is set to 1024. This parameter has no effect prior to CDH 4.4.

Related Name

mapreduce.reduce.memory.mb

Default Value

0 B

API Name

mapreduce_reduce_memory_mb

Required

false

ApplicationMaster Java Maximum Heap Size

Description

The maximum heap size, in bytes, of the Java MapReduce ApplicationMaster. This number will be formatted and concatenated with 'ApplicationMaster Java Opts Base' to pass to Hadoop.

Related Name

Default Value

825955249 B

API Name

yarn_app_mapreduce_am_max_heap

Required

false

ApplicationMaster Virtual CPU Cores

Description

The virtual CPU cores requirement, for the ApplicationMaster. This parameter has no effect prior to CDH 4.4.

Related Name

yarn.app.mapreduce.am.resource.cpu-vcores

Default Value

1

API Name

yarn_app_mapreduce_am_resource_cpu_vcores

Required

false

ApplicationMaster Memory

Description

The physical memory requirement, in MiB, for the ApplicationMaster.

Related Name

yarn.app.mapreduce.am.resource.mb

Default Value

1 GiB

API Name

yarn_app_mapreduce_am_resource_mb

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Deploy Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Deploy Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Parameter Validation: Running Job History Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Running Job History Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_job_history_dir

Required

true

Suppress Parameter Validation: I/O Sort Factor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the I/O Sort Factor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_io_sort_factor

Required

true

Suppress Parameter Validation: Gateway Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Compression Codec of MapReduce Map Output

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Compression Codec of MapReduce Map Output parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_map_output_compression_codec

Required

true

Suppress Parameter Validation: Compression Codec of MapReduce Job Output

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Compression Codec of MapReduce Job Output parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_output_compression_codec

Required

true

Suppress Parameter Validation: MR Application Environment

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MR Application Environment parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_admin_user_env

Required

true

Suppress Parameter Validation: Maximum Number of Attempts for MapReduce Jobs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Maximum Number of Attempts for MapReduce Jobs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_am_max_attempts

Required

true

Suppress Parameter Validation: MR Application Classpath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MR Application Classpath parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_application_classpath

Required

true

Suppress Parameter Validation: MR Application Framework Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MR Application Framework Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_application_framework_path

Required

true

Suppress Parameter Validation: MapReduce Client Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce Client Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_config_safety_valve

Required

true

Suppress Parameter Validation: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_env_safety_valve

Required

true

Suppress Parameter Validation: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Java Configuration Options parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_java_opts

Required

true

Suppress Parameter Validation: ACL For Modifying A Job

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ACL For Modifying A Job parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_acl_modify_job

Required

true

Suppress Parameter Validation: ACL For Viewing A Job

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ACL For Viewing A Job parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_acl_view_job

Required

true

Suppress Parameter Validation: Redacted MapReduce Job Properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Redacted MapReduce Job Properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_redacted_properties

Required

true

Suppress Parameter Validation: Map Task Java Opts Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Map Task Java Opts Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_map_java_opts

Required

true

Suppress Configuration Validator: Map Task Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Map Task Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_map_java_opts_max_heap_mapreduce_map_memory_mb_validator

Required

true

Suppress Parameter Validation: Reduce Task Java Opts Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reduce Task Java Opts Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_reduce_java_opts

Required

true

Suppress Configuration Validator: Reduce Task Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Reduce Task Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_reduce_java_opts_max_heap_mapreduce_reduce_memory_mb_validator

Required

true

Suppress Configuration Validator: Job Submit Replication Validator

Description

Whether to suppress configuration warnings produced by the Job Submit Replication Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_replication_validator

Required

true

Suppress Parameter Validation: ApplicationMaster Environment

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ApplicationMaster Environment parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_admin_user_env

Required

true

Suppress Parameter Validation: ApplicationMaster Java Opts Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ApplicationMaster Java Opts Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_command_opts

Required

true

Suppress Configuration Validator: ApplicationMaster Java Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the ApplicationMaster Java Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_max_heap_yarn_app_mapreduce_am_resource_mb_validator

Required

true

Suppress Parameter Validation: YARN Client Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Client Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_client_config_safety_valve

Required

true

JobHistory Server

Advanced

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

System Group

Description

The group that the JobHistory Server process should run as.

Related Name

Default Value

hadoop

API Name

history_process_groupname

Required

true

System User

Description

The user that the JobHistory Server process should run as.

Related Name

Default Value

mapred

API Name

history_process_username

Required

true

JobHistory Server Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only. A string to be inserted into yarn-site.xml for this role only.

Related Name

Default Value

API Name

jobhistory_config_safety_valve

Required

false

JobHistory Server Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only. A string to be inserted into mapred-site.xml for this role only.

Related Name

Default Value

API Name

jobhistory_mapred_safety_valve

Required

false

JobHistory Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

JOBHISTORY_role_env_safety_valve

Required

false

JobHistory Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Java Configuration Options for JobHistory Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or

greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS -Dlibrary.leveldbjni.path=CMF_CONF_DIR

API Name

mr2_jobhistory_java_opts

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

JobHistory Server Logging Threshold

Description

The minimum log level for JobHistory Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

JobHistory Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for JobHistory Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

JobHistory Server Max Log Size

Description

The maximum size, in megabytes, per log file for JobHistory Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

JobHistory Server Log Directory

Description

Directory where JobHistory Server will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-mapreduce

API Name

mr2_jobhistory_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11132

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

jobhistory_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

jobhistory_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

jobhistory_gc_duration_window

Required

false

JobHistory Server Host Health Test

Description

When computing the overall JobHistory Server health, consider the host's health.

Related Name

Default Value

true

API Name

jobhistory_host_health_enabled

Required

false

JobHistory Server Process Health Test

Description

Enables the health test that the JobHistory Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

jobhistory_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

jobhistory_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

jobhistory_web_metric_collection_thresholds

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.

- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting

#log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Job ACL

Description

Specifies whether ACLs should be checked for authorization when users perform various operations. If enabled, access control checks are made by MapReduce when requests are made by users for queue operations and job operations. Queue operations include submitting job to a queue or killing a job in the queue. Job operations include viewing the job-details (See mapreduce.job.acl-view-job), or modifying a job (See mapreduce.job.acl-modify-job).

Related Name

mapreduce.cluster.acls.enabled

Default Value

false

API Name

mapreduce_cluster_acls_enabled

Required

false

Job History Files Cleaner Interval

Description

Time interval for history cleaner to check for files to delete. Files are only deleted if they are older than mapreduce.jobhistory.max-age-ms.

Related Name

mapreduce.jobhistory.cleaner.interval

Default Value

1 day(s)

API Name

mapreduce_jobhistory_cleaner_interval

Required

false

Job History Files Maximum Age

Description

Job history files older than this time duration will deleted when the history cleaner runs.

Related Name

mapreduce.jobhistory.max-age-ms

Default Value

7 day(s)

API Name

mapreduce_jobhistory_max_age_ms

Required

false

Max Shuffle Connections

Description

Maximum allowed connections for the shuffle. Set to 0 (zero) to indicate no limit on the number of connections.

Related Name

mapreduce.jobhistory.loadedjob.tasks.max

Default Value

-1

API Name

mapreduce_shuffle_max_connections

Required

false

MapReduce ApplicationMaster Staging Root Directory

Description

The root HDFS directory of the staging area for users' MR2 jobs; for example /user. The staging directories are always named after the user.

Related Name

yarn.app.mapreduce.am.staging-dir

Default Value

/user

API Name

yarn_app_mapreduce_am_staging_dir

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

MapReduce JobHistory Server Port

Description

The port of the MapReduce JobHistory Server. Together with the hostname of the JobHistory role, forms the address.

Related Name

mapreduce.jobhistory.address

Default Value

10020

API Name

mapreduce_jobhistory_address

Required

false

MapReduce JobHistory Server Admin Interface Port

Description

The port of the MapReduce JobHistory Server administrative interface. Together with the host name of the JobHistory role forms the address.

Related Name

mapreduce.jobhistory.admin.address

Default Value

10033

API Name

mapreduce_jobhistory_admin_address

Required

false

MapReduce JobHistory Web Application HTTP Port

Description

The HTTP port of the MapReduce JobHistory Server web application. Together with the host name of the JobHistory role forms the address.

Related Name

mapreduce.jobhistory.webapp.address

Default Value

19888

API Name

mapreduce_jobhistory_webapp_address

Required

false

MapReduce JobHistory Web Application HTTPS Port (TLS/SSL)

Description

The HTTPS port of the MapReduce JobHistory Server web application. Together with the host name of the JobHistory role forms the address.

Related Name

mapreduce.jobhistory.webapp.https.address

Default Value

19890

API Name

mapreduce_jobhistory_webapp_https_address

Required

false

Bind JobHistory Server to Wildcard Address

Description

If enabled, the JobHistory Server binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

yarn_jobhistory_bind_wildcard

Required

false

Resource Management

Java Heap Size of JobHistory Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

mr2_jobhistory_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the JobHistory Server roles.

Related Name

Default Value

mapred

API Name

kerberos_role_princ_name

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_history_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_history_process_username

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: JobHistory Server Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobHistory Server Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_config_safety_valve

Required

true

Suppress Parameter Validation: JobHistory Server Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobHistory Server Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_mapred_safety_valve

Required

true

Suppress Parameter Validation: JobHistory Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobHistory Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_role_env_safety_valve

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: JobHistory Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobHistory Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: MapReduce JobHistory Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce JobHistory Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_address

Required

true

Suppress Parameter Validation: MapReduce JobHistory Server Admin Interface Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce JobHistory Server Admin Interface Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_admin_address

Required

true

Suppress Parameter Validation: MapReduce JobHistory Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce JobHistory Web Application HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_webapp_address

Required

true

Suppress Parameter Validation: MapReduce JobHistory Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce JobHistory Web Application HTTPS Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_webapp_https_address

Required

true

Suppress Parameter Validation: Java Configuration Options for JobHistory Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for JobHistory Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mr2_jobhistory_java_opts

Required

true

Suppress Parameter Validation: JobHistory Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JobHistory Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mr2_jobhistory_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: MapReduce ApplicationMaster Staging Root Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the MapReduce ApplicationMaster Staging Root Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_staging_dir

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_jobhistory_web_metric_collection

Required

true

NodeManager

Advanced

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

CGroups Hierarchy

Description

Path (rooted in the cgroups hierarchy on the machine) where to place YARN-managed cgroups.

Related Name

yarn.nodemanager.linux-container-executor.cgroups.hierarchy

Default Value

/hadoop-yarn

API Name

linux_container_executor_cgroups_hierarchy

Required

false

NodeManager Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Healthchecker Script Arguments

Description

Comma-separated list of arguments which are to be passed to node health script when it is being launched.

Related Name

yarn.nodemanager.health-checker.script.opts

Default Value

API Name

mapred_healthchecker_script_args

Required

false

Healthchecker Script Path

Description

Absolute path to the script which is periodically run by the node health monitoring service to determine if the node is healthy or not. If the value of this key is empty or the file does not exist in the location configured here, the node health monitoring service is not started.

Related Name

yarn.nodemanager.health-checker.script.path

Default Value

API Name

mapred_healthchecker_script_path

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Java Configuration Options for NodeManager

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS -Dlibrary.leveldbjni.path=CMF_CONF_DIR

API Name

node_manager_java_opts

Required

false

NodeManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only. A string to be inserted into yarn-site.xml for this role only.

Related Name

Default Value

API Name

nodemanager_config_safety_valve

Required

false

Enable Container Launch Debug Information

Description

Generate additional logs about container launches for e.g. a copy of the launch script and lists the directory contents of the container work dir also following symlinks to a max-depth of 5.

Related Name

yarn.nodemanager.log-container-debug-info.enabled

Default Value

false

API Name

nodemanager_log_container_debug_info_enabled

Required

false

NodeManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only. A string to be inserted into mapred-site.xml for this role only.

Related Name

Default Value

API Name

nodemanager_mapred_safety_valve

Required

false

NodeManager Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

NODEMANAGER_role_env_safety_valve

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Localized Dir Deletion Delay

Description

Number of seconds after an application finishes before the NodeManager's DeletionService will delete the application's localized file and log directory. To diagnose YARN application problems, set this property's value large enough (for example, to 600 = 10 minutes) to permit examination of these directories.

Related Name

yarn.nodemanager.delete.debug-delay-sec

Default Value

0

API Name

yarn_nodemanager_delete_debug_delay_sec

Required

false

Disk Health Checker Disk Utilization Watermark Low Threshold Percentage

Description

The low threshold percentage of disk space used when a bad disk is marked as good. Values can range from 0.0 to 100.0. This applies to yarn.nodemanager.local-dirs and yarn.nodemanager.log-dirs. Note that if its value is more than yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage or not set, it will be set to the same value as yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage.

Related Name

yarn.nodemanager.disk-health-checker.disk-utilization-watermark-low-per-disk-percentage

Default Value

API Name

yarn_nodemanager_disk_health_checker_disk_utilization_watermark_low_per_disk_percentage

Required

false

Disk Health Checker Frequency

Description

Frequency, in milliseconds, of running disk health checker.

Related Name

yarn.nodemanager.disk-health-checker.interval-ms

Default Value

2 minute(s)

API Name

yarn_nodemanager_disk_health_checker_interval_ms

Required

false

Dish Health Checker Max Disk Utilization Percent

Description

The maximum percentage of disk space utilization allowed after which a disk is marked as bad. Values can range from 0.0 to 100.0. If the value is greater than or equal to 100, the NodeManager will check for full disk. This applies to local directories and log directories.

Related Name

yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage

Default Value

90.0 %

API Name

yarn_nodemanager_disk_health_checker_max_disk_utilization_per_disk_percentage

Required

false

Disk Health Checker Minimum Health Disk Space

Description

The minimum space that must be available on a disk for it to be used. This applies to local directories and log directories.

Related Name

yarn.nodemanager.disk-health-checker.min-free-space-per-disk-mb

Default Value

0 B

API Name

yarn_nodemanager_disk_health_checker_min_free_space_per_disk_mb

Required

false

Disk Health Checker Minimum Health Disks Fraction

Description

The minimum fraction of number of disks to be healthy for the NodeManager to launch new containers. This correspond to both local directories and log directories; that is, if there are fewer healthy local directories (or log directories) available, then new containers will not be launched on this node.

Related Name

yarn.nodemanager.disk-health-checker.min-healthy-disks

Default Value

0.25

API Name

yarn_nodemanager_disk_health_checker_min_healthy_disks

Required

false

Docker on YARN

Enable Docker Containers

Description

Specifies if Docker containers in YARN are enabled.

Related Name

Default Value

false

API Name

docker_on_yarn_enabled

Required

false

Allowed Devices for Docker Containers

Description

Specifies the devices that Docker containers are allowed to mount. By default, no devices are allowed to be mounted.

Related Name

docker.allowed.devices

Default Value

API Name

yarn_docker_allowed_devices

Required

false

Allowed Read-Only Mounts for Docker Containers

Description

Specifies the directories that Docker containers are allowed to mount in read-only mode. NodeManager Local Directories and Cgroups root are always added to this list. Ensure that any additional default read-only mounts are also added here.

Related Name

docker.allowed.ro-mounts

Default Value

API Name

yarn_docker_allowed_ro_mounts

Required

false

Allowed Read-Write Mounts for Docker Containers

Description

Specifies the directories that Docker containers are allowed to mount in read-write mode. NodeManager Local Directories and NodeManager Container Log Directories are always added to this list. Ensure that any additional default read-write mounts are also added here.

Related Name

docker.allowed.rw-mounts

Default Value

API Name

yarn_docker_allowed_rw_mounts

Required

false

Allowed Volume Drivers for Docker Containers

Description

Specifies the volume drivers which are alllowed to be used with Docker. By default, no volume drivers are allowed.

Related Name

docker.allowed.volume-drivers

Default Value

API Name

yarn_docker_allowed_volume_drivers

Required

false

Docker Binary Path

Description

Specifies the path of the binary in the hosts that is used to launch Docker containers. Its default value is /usr/bin/docker.

Related Name

docker.binary

Default Value

/usr/bin/docker

API Name

yarn_docker_binary

Required

false

Enable No-new-privileges Flag for Docker Containers

Description

Specifies if the no-new-privileges flag for docker run is enabled. The no-new-privileges flag ensures that the process or its children processes do not gain any additional privileges. Set to 'true' to enable.

Related Name

docker.no-new-privileges.enabled

Default Value

false

API Name

yarn_docker_no_new_privileges_enabled

Required

false

Trusted Registries for Docker Containers

Description

Specifies the list of trusted docker registries for running trusted docker containers. By default, no registries are defined.

Related Name

docker.trusted.registries

Default Value

API Name

yarn_docker_trusted_registries

Required

false

Allowed Docker Container Networks

Description

Specifies the networks that are allowed for Docker containers. Valid values are determined by Docker networks available from the docker network ls command.

Related Name

yarn.nodemanager.runtime.linux.docker.allowed-container-networks

Default Value

host none bridge

API Name

yarn_nodemanager_runtime_linux_docker_allowed_container_networks

Required

false

Docker Capabilities

Description

Specifies the capabilities assigned to Docker containers when they are launched. The values may not be case-sensitive from a docker perspective, but Cloudera recommends to keep them uppercase.

Related Name

yarn.nodemanager.runtime.linux.docker.capabilities

Default Value

CHOWN, DAC_OVERRIDE, FSETID, FOWNER, MKNOD, NET_RAW, SETGID, SETUID, SETFCAP, SETPCAP, NET_BIND_SERVICE, SYS_CHROOT, KILL, AUDIT_WRITE

API Name

yarn_nodemanager_runtime_linux_docker_capabilities

Required

false

Default Docker Container Network

Description

Specifies which allowed network is used when launching Docker containers but no network is specified in the request. This network must be added to yarn.nodemanager.runtime.linux.docker.allowed-container-networks.

Related Name

yarn.nodemanager.runtime.linux.docker.default-container-network

Default Value

host

API Name

yarn_nodemanager_runtime_linux_docker_default_container_network

Required

false

Default Read-Only Mounts for Docker Containers

Description

A list that specifies the default read-only mounts to be bind-mounted into all Docker containers that use DockerContainerRuntime. NodeManager Local Directories and Cgroups root are always added to this list. Ensure that any additional default read-only mounts are also added to the Allowed Read-Only Mounts list.

Related Name

yarn.nodemanager.runtime.linux.docker.default-ro-mounts

Default Value

API Name

yarn_nodemanager_runtime_linux_docker_default_ro_mounts

Required

false

Default Read-Write Mounts for Docker Containers

Description

A list that specifies the default read-write mounts to be bind-mounted into all Docker containers that use DockerContainerRuntime. NodeManager Local Directories and NodeManager Container Log Directories are always added to this list. Ensure that any additional default read-write mounts are also added to the Allowed Read-Write Mounts list.

Related Name

yarn.nodemanager.runtime.linux.docker.default-rw-mounts

Default Value

API Name

yarn_nodemanager_runtime_linux_docker_default_rw_mounts

Required

false

Default Tempfs Mounts for Docker Containers

Description

Specifies the directories in tmpfs that Docker containers are allowed to mount. By default, no directories are allowed in tmpfs to be mounted.

Related Name

yarn.nodemanager.runtime.linux.docker.default-tmpfs-mounts

Default Value

API Name

yarn_nodemanager_runtime_linux_docker_default_tmpfs_mounts

Required

false

Allow Delayed Removal of Docker Containers

Description

Specifies if Debug Deletion Delay is used for Docker containers. Debug Deletion Delay is useful for troubleshooting Docker container related launch failures. For more information, see yarn.nodemanager.delete.debug-delay-sec.

Related Name

yarn.nodemanager.runtime.linux.docker.delayed-removal.allowed

Default Value

false

API Name

yarn_nodemanager_runtime_linux_docker_delayed_removal_allowed

Required

false

Enable User Remapping for Docker Containers

Description

Specifies if Docker containers can run with the UID (User Identifier) and GID (Group Identifier) of the calling user.

Related Name

yarn.nodemanager.runtime.linux.docker.enable-userremapping.allowed

Default Value

true

API Name

yarn_nodemanager_runtime_linux_docker_enable_userremapping_allowed

Required

false

Allow Using Host PID Namespace for Docker Containers

Description

Specifies if Docker containers are allowed to use the host PID namespace.

Related Name

yarn.nodemanager.runtime.linux.docker.host-pid-namespace.allowed

Default Value

false

API Name

yarn_nodemanager_runtime_linux_docker_host_pid_namespace_allowed

Required

false

ACL for Privileged Docker Containers

Description

A comma-separated list that specifies the users who can request privileged Docker containers if privileged Docker containers are allowed.

Related Name

yarn.nodemanager.runtime.linux.docker.privileged-containers.acl

Default Value

API Name

yarn_nodemanager_runtime_linux_docker_privileged_containers_acl

Required

false

Allow Privileged Docker Containers

Description

Specifies if applications are allowed to run in privileged containers. Privileged containers are granted the complete set of capabilities and are not subject to the limitations imposed by the device cgroup controller. Use with extreme care!

Related Name

yarn.nodemanager.runtime.linux.docker.privileged-containers.allowed

Default Value

false

API Name

yarn_nodemanager_runtime_linux_docker_privileged_containers_allowed

Required

false

User Remapping GID Threshold for Docker Containers

Description

Specifies the minimum GID (Group Identifier) for a remapped user. Users with GIDs lower then this minimum value are not allowed to launch Docker containers when user remapping (yarn.nodemanager.runtime.linux.docker.enable-userremapping.allowed) is enabled.

Related Name

yarn.nodemanager.runtime.linux.docker.userremapping-gid-threshold

Default Value

1

API Name

yarn_nodemanager_runtime_linux_docker_userremapping_gid_threshold

Required

false

User Remapping UID Threshold for Docker Containers

Description

Specifies the minimum UID (User Identifier) for a remapped user. Users with UIDs lower than this minimum value are not allowed to launch Docker containers when user remapping (yarn.nodemanager.runtime.linux.docker.enable-userremapping.allowed) is enabled.

Related Name

yarn.nodemanager.runtime.linux.docker.userremapping-uid-threshold

Default Value

1

API Name

yarn_nodemanager_runtime_linux_docker_userremapping_uid_threshold

Required

false

FPGA Management

Enable FPGA Usage

Description

Allows NodeManagers to provide FPGA devices to YARN applications that request them.

Related Name

yarn.nodemanager.fpga_enabled

Default Value

false

API Name

yarn_nodemanager_fpga_enabled

Required

false

FPGA device major number

Description

The major device number of the FPGA card

Related Name

yarn.nodemanager.fpga_major_device_number

Default Value

238

API Name

yarn_nodemanager_fpga_major_device_number

Required

false

FPGA initializer script

Description

The shell script which sets up the environment for the FPGA device. It is usually a short shell script which sources other scripts and exports environment variables.

Related Name

yarn.nodemanager.fpga_plugin_initializer_script

Default Value

API Name

yarn_nodemanager_fpga_plugin_initializer_script

Required

false

Allowed FPGA devices

Description

Specifies FPGA devices which can be managed by YARN NodeManager (in a comma-separated list). Manually specify FPGA devices if you only want a subset of FPGA devices to be managed

by YARN. An FPGA device is identified by the minor device number. An example of manual specification is "0,1" to allow YARN NodeManager to manage FPGA devices with minor numbers 0/1. Default is "auto", which allows all devices.

Related Name

yarn.nodemanager.resource-plugins.fpga.allowed-fpga-devices

Default Value

auto

API Name

yarn_nodemanager_resource_plugins_fpga_allowed_fpga_devices

Required

false

List of available FPGA devices

Description

Specifies the available FPGA devices in a given format: deviceA/N:M,deviceB/X:Y. Example: acl0/243:0,acl1/243:1. The numbers after the "/" character are the device major and minor numbers.

Related Name

yarn.nodemanager.resource-plugins.fpga.available-devices

Default Value

API Name

yarn_nodemanager_resource_plugins_fpga_available_devices

Required

false

Path to FPGA (aocl) tool

Description

Full local path to the Intel "aocl" tool installed on the node.

Related Name

yarn.nodemanager.resource-plugins.fpga.path-to-discovery-executables

Default Value

API Name

yarn_nodemanager_resource_plugins_fpga_path_to_discovery_executables

Required

false

GPU Management

Enable GPU Usage

Description

Allows NodeManagers to provide GPU devices to YARN applications that request them.

Related Name

Default Value

false

API Name

gpu_enabled

Required

false

NodeManager GPU Devices Allowed

Description

Specifies GPU devices which can be managed by YARN NodeManager (comma-separated). Manually specify GPU devices if auto detection of GPU devices failed or you only want a subset of GPU devices to be managed by YARN. A GPU device is identified by the minor device number and index: An example of manual specification is "0:0,1:1,2:2,3:4" to allow YARN NodeManager to manage GPU devices with indices 0/1/2/3 and minor number 0/1/2/4 numbers.

Related Name

yarn.nodemanager.resource-plugins.gpu.allowed-gpu-devices

Default Value

auto

API Name

gpu_plugin_allowed_devices

Required

false

NodeManager GPU Detection Executable

Description

Path to the executable program which YARN runs to get GPU-related information. When this value is empty (default), YARN NodeManager will try to locate the executable itself. An example value is: /usr/local/bin/nvidia-smi

Related Name

yarn.nodemanager.resource-plugins.gpu.path-to-discovery-executables

Default Value

API Name

gpu_plugin_detector_path

Required

false

Log Aggregation

Log Aggregation Policy

Description

Specifies the types of container logs that are uploaded during the log aggregation.

Related Name

yarn.nodemanager.log-aggregation.policy.class

Default Value

org.apache.hadoop.yarn.server.nodemanager.containermanager.logaggregation.AllContainerLogAggregationPolicy

API Name

yarn_nodemanager_log_aggregation_policy_class

Required

false

Log Aggregation Roll Monitoring Interval

Description

Defines how often NodeManagers wake up to upload log files. If this value is 0 or less than 0, the logs are uploaded when the application is completed.

Related Name

yarn.nodemanager.log-aggregation.roll-monitoring-interval-seconds

Default Value

-1 second(s)

API Name

yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds

Required

false

Minimum Hard Limit for Log Aggregation Roll Monitoring Interval

Description

Defines the hard minimum value for yarn.nodemanager.log-aggregation.roll-monitoring-interval-seconds, if Log Aggregation Roll Monitoring Interval has been set to a positive value.

Related Name

yarn.nodemanager.log-aggregation.roll-monitoring-interval-seconds.min

Default Value

1 hour(s)

API Name

yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds_min

Required

false

Remote App Log Directory

Description

Specifies the path of the directory where application logs are stored after an application is completed.

Related Name

yarn.nodemanager.remote-app-log-dir

Default Value

/tmp/logs

API Name

yarn_nodemanager_remote_app_log_dir

Required

false

Remote App Log Directory Suffix

Description

The remote log directory is created at {yarn.nodemanager.remote-app-log-dir}/${user}/{thisParam}

Related Name

yarn.nodemanager.remote-app-log-dir-suffix

Default Value

logs

API Name

yarn_nodemanager_remote_app_log_dir_suffix

Required

false

Logs

NodeManager Logging Threshold

Description

The minimum log level for NodeManager logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

NodeManager Maximum Log File Backups

Description

The maximum number of rolled log files to keep for NodeManager logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

NodeManager Max Log Size

Description

The maximum size, in megabytes, per log file for NodeManager logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

NodeManager Log Directory

Description

Directory where NodeManager will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-yarn

API Name

node_manager_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11131

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.

- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

NodeManager Connectivity Health Check

Description

Enables the health check that verifies the NodeManager is connected to the ResourceManager.

Related Name

Default Value

true

API Name

nodemanager_connectivity_health_enabled

Required

false

NodeManager Connectivity Tolerance at Startup

Description

The amount of time to wait for the NodeManager to fully start up and connect to the ResourceManager before enforcing the connectivity check.

Related Name

Default Value

3 minute(s)

API Name

nodemanager_connectivity_tolerance_seconds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

nodemanager_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

nodemanager_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

nodemanager_gc_duration_window

Required

false

NodeManager Health Checker Health Check

Description

Enables the health check that verifies the NodeManager is seen as healthy by the ResourceManager.

Related Name

Default Value

true

API Name

nodemanager_health_checker_health_enabled

Required

false

NodeManager Host Health Test

Description

When computing the overall NodeManager health, consider the host's health.

Related Name

Default Value

true

API Name

nodemanager_host_health_enabled

Required

false

NodeManager Local Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Local Directories.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

nodemanager_local_data_directories_free_space_absolute_thresholds

Required

false

NodeManager Local Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Local Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Local Directories Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

nodemanager_local_data_directories_free_space_percentage_thresholds

Required

false

NodeManager Container Log Directories Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Container Log Directories.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

nodemanager_log_directories_free_space_absolute_thresholds

Required

false

NodeManager Container Log Directories Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Container Log Directories. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Container Log Directories Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

nodemanager_log_directories_free_space_percentage_thresholds

Required

false

NodeManager Recovery Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Recovery Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

nodemanager_recovery_directory_free_space_absolute_thresholds

Required

false

NodeManager Recovery Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's NodeManager Recovery Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a NodeManager Recovery Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

nodemanager_recovery_directory_free_space_percentage_thresholds

Required

false

NodeManager Process Health Test

Description

Enables the health test that the NodeManager's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

nodemanager_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

nodemanager_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

nodemanager_web_metric_collection_thresholds

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn: $INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Enable Shuffle Auxiliary Service

Description

If enabled, adds 'org.apache.hadoop.mapred.ShuffleHandler' to the NodeManager auxiliary services. This is required for MapReduce applications.

Related Name

Default Value

true

API Name

mapreduce_aux_service

Required

false

Support for keep-alive connections

Description

Enable support for keep-alive connections. Set to true to support keep-alive connections.

Related Name

mapreduce.shuffle.connection-keep-alive.enable

Default Value

true

API Name

mapreduce_shuffle_connection_keep_alive_enable

Required

false

Max Shuffle Connections

Description

Maximum allowed connections for the shuffle. Set to 0 (zero) to indicate no limit on the number of connections.

Related Name

mapreduce.shuffle.max.connections

Default Value

0

API Name

mapreduce_shuffle_max_connections

Required

false

Containers Environment Variable

Description

Environment variables that should be forwarded from the NodeManager's environment to the container's.

Related Name

yarn.nodemanager.admin-env

Default Value

MALLOC_ARENA_MAX=$MALLOC_ARENA_MAX

API Name

yarn_nodemanager_admin_env

Required

false

Container Manager Thread Count

Description

Number of threads container manager uses.

Related Name

yarn.nodemanager.container-manager.thread-count

Default Value

20

API Name

yarn_nodemanager_container_manager_thread_count

Required

false

Cleanup Thread Count

Description

Number of threads used in cleanup.

Related Name

yarn.nodemanager.delete.thread-count

Default Value

4

API Name

yarn_nodemanager_delete_thread_count

Required

false

Containers Environment Variables Whitelist

Description

Environment variables that containers may override rather than use NodeManager's default.

Related Name

yarn.nodemanager.env-whitelist

Default Value

JAVA_HOME, HADOOP_COMMON_HOME, HADOOP_HDFS_HOME, HADOOP_CLIENT_CONF_DIR, HADOOP_YARN_HOME, HADOOP_MAPRED_HOME, MR2_CLASSPATH, JAVA_LIBRARY_PATH, HADOOP_HOME, PATH, LANG, TZ

API Name

yarn_nodemanager_env_whitelist

Required

false

Heartbeat Interval

Description

Heartbeat interval to ResourceManager

Related Name

yarn.resourcemanager.nodemanagers.heartbeat-interval-ms

Default Value

1 second(s)

API Name

yarn_nodemanager_heartbeat_interval_ms

Required

false

NodeManager Local Directories

Description

List of directories on the local filesystem where a NodeManager stores intermediate data files.

Related Name

yarn.nodemanager.local-dirs

Default Value

API Name

yarn_nodemanager_local_dirs

Required

true

Localizer Cache Cleanup Interval

Description

Address where the localizer IPC is.

Related Name

yarn.nodemanager.localizer.cache.cleanup.interval-ms

Default Value

10 minute(s)

API Name

yarn_nodemanager_localizer_cache_cleanup_interval_ms

Required

false

Localizer Cache Target Size

Description

Target size of localizer cache in MB, per local directory.

Related Name

yarn.nodemanager.localizer.cache.target-size-mb

Default Value

10 GiB

API Name

yarn_nodemanager_localizer_cache_target_size_mb

Required

false

Localizer Client Thread Count

Description

Number of threads to handle localization requests.

Related Name

yarn.nodemanager.localizer.client.thread-count

Default Value

5

API Name

yarn_nodemanager_localizer_client_thread_count

Required

false

Localizer Fetch Thread Count

Description

Number of threads to use for localization fetching.

Related Name

yarn.nodemanager.localizer.fetch.thread-count

Default Value

4

API Name

yarn_nodemanager_localizer_fetch_thread_count

Required

false

NodeManager Container Log Directories

Description

List of directories on the local filesystem where a NodeManager stores container log files.

Related Name

yarn.nodemanager.log-dirs

Default Value

/var/log/hadoop-yarn/container

API Name

yarn_nodemanager_log_dirs

Required

true

Log Retain Duration

Description

Time in seconds to retain user logs. Only applicable if log aggregation is disabled.

Related Name

yarn.nodemanager.log.retain-seconds

Default Value

3 hour(s)

API Name

yarn_nodemanager_log_retain_seconds

Required

false

NodeManager Recovery Directory

Description

The local filesystem directory in which the NodeManager stores state when recovery is enabled. Recovery is enabled by default.

Related Name

yarn.nodemanager.recovery.dir

Default Value

/var/lib/hadoop-yarn/yarn-nm-recovery

API Name

yarn_nodemanager_recovery_dir

Required

false

Enable NodeManager Recovery

Description

When enabled, any applications that were running on the cluster before the NodeManager was restarted or died will be recovered after the NodeManager is restarted. Recovery is enabled by default.

Related Name

yarn.nodemanager.recovery.enabled

Default Value

true

API Name

yarn_nodemanager_recovery_enabled

Required

false

Enable NodeManager Supervision under Recovery

Description

When enabled, the NodeManager running will not try to cleanup containers as it exits with the assumption it will be immediately restarted and recover containers. Supervision is enabled by default.

Related Name

yarn.nodemanager.recovery.supervised

Default Value

true

API Name

yarn_nodemanager_recovery_supervised

Required

false

Allowed Linux Runtimes

Description

Specifies the runtimes that are allowed when LinuxContainerExecutor is used.

Related Name

yarn.nodemanager.runtime.linux.allowed-runtimes

Default Value

default

API Name

yarn_nodemanager_runtime_linux_allowed_runtimes

Required

false

Sleep Delay Before SIGKILL

Description

Specifies the time in milliseconds between sending a SIGTERM and a SIGKILL signal to a running container.

Related Name

yarn.nodemanager.sleep-delay-before-sigkill.ms

Default Value

10 millisecond(s)

API Name

yarn_nodemanager_sleep_delay_before_sigkill_ms

Required

false

Performance

Max Shuffle Threads

Description

Maximum allowed threads for serving shuffle connections. Set to zero to indicate the default of 2 times the number of available processors.

Related Name

mapreduce.shuffle.max.threads

Default Value

80

API Name

mapreduce_shuffle_max_threads

Required

false

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

NodeManager Web Application HTTPS Port (TLS/SSL)

Description

The HTTPS port of the NodeManager web application.

Related Name

yarn.nodemanager.webapp.https.address

Default Value

8044

API Name

nodemanager_webserver_https_port

Required

false

NodeManager Web Application HTTP Port

Description

The HTTP Port of the NodeManager web application.

Related Name

yarn.nodemanager.webapp.address

Default Value

8042

API Name

nodemanager_webserver_port

Required

false

NodeManager IPC Address

Description

The address of the NodeManager IPC.

Related Name

yarn.nodemanager.address

Default Value

8041

API Name

yarn_nodemanager_address

Required

false

Localizer Port

Description

Address where the localizer IPC is.

Related Name

yarn.nodemanager.localizer.address

Default Value

8040

API Name

yarn_nodemanager_localizer_address

Required

false

Resource Management

Java Heap Size of NodeManager in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

node_manager_java_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Strict CGroup Resource Usage

Description

CGroups allows cpu usage limits to be hard or soft. When this setting is true, containers cannot use more CPU usage than allocated even if spare CPU is available. This ensures that containers can only use CPU that they were allocated. When set to false, containers can use spare CPU if available. It should be noted that irrespective of whether set to true or false, at no time can the combined CPU usage of all containers exceed the value specified in Containers CPU Limit Percentage.

Related Name

yarn.nodemanager.linux-container-executor.cgroups.strict-resource-usage

Default Value

false

API Name

yarn_nodemanager_linux_container_executor_cgroups_strict_resource_usage

Required

false

Container Virtual CPU Cores

Description

Number of virtual CPU cores that can be allocated for containers. This parameter has no effect prior to CDH 4.4.

Related Name

yarn.nodemanager.resource.cpu-vcores

Default Value

8

API Name

yarn_nodemanager_resource_cpu_vcores

Required

true

Container Memory

Description

Amount of physical memory, in MiB, that can be allocated for containers.

Related Name

yarn.nodemanager.resource.memory-mb

Default Value

8 GiB

API Name

yarn_nodemanager_resource_memory_mb

Required

true

Containers CPU Limit Percentage

Description

Amount of CPU reserved for all the containers on each node.

Related Name

yarn.nodemanager.resource.percentage-physical-cpu-limit

Default Value

100

API Name

yarn_nodemanager_resource_percentage_physical_cpu_limit

Required

false

Enable Virtual Memory Check

Description

Enforce virtual memory limit on containers, given as a ratio to physical memory.

Related Name

yarn.nodemanager.vmem-check-enabled

Default Value

false

API Name

yarn_nodemanager_vmem_check_enabled

Required

false

Virtual Memory to Physical Memory Ratio

Description

Ratio between virtual memory to physical memory when setting yarn.nodemanager.vmem-check-enabled to true. Container allocations are expressed in terms of physical memory, and virtual memory usage is allowed to exceed this allocation by this ratio. At least 2.1 is suggested to be set.

Related Name

yarn.nodemanager.vmem-pmem-ratio

Default Value

2.1

API Name

yarn_nodemanager_vmem_pmem_ratio

Required

false

Resource Types

Resource Allocations

Description

Each NodeManager can independently define the resources that are available from that node.

Related Name

Default Value

API Name

resource_allocations

Required

false

Security

Allowed System Users

Description

List of users explicitly whitelisted to be allowed to run containers. Users with IDs lower than the "Minimum User Id" setting may be whitelisted by using this setting.

Related Name

allowed.system.users

Default Value

nobody impala hive llama hbase

API Name

container_executor_allowed_system_users

Required

false

Banned System Users

Description

List of users banned from running containers.

Related Name

banned.users

Default Value

hdfs yarn mapred bin

API Name

container_executor_banned_users

Required

false

Container Executor Group

Description

The system group that owns the container-executor binary. This does not need to be changed unless the ownership of the binary is explicitly changed.

Related Name

yarn.nodemanager.linux-container-executor.group

Default Value

yarn

API Name

container_executor_group

Required

false

Minimum User ID

Description

The minimum Linux user ID allowed. Used to prevent other super users.

Related Name

min.user.id

Default Value

1000

API Name

container_executor_min_user_id

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Allowed System Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed System Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_allowed_system_users

Required

true

Suppress Parameter Validation: Banned System Users

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Banned System Users parameter.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_banned_users

Required

true

Suppress Parameter Validation: Container Executor Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Executor Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_group

Required

true

Suppress Parameter Validation: NodeManager GPU Devices Allowed

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager GPU Devices Allowed parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gpu_plugin_allowed_devices

Required

true

Suppress Parameter Validation: NodeManager GPU Detection Executable

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager GPU Detection Executable parameter.

Related Name

Default Value

false

API Name

role_config_suppression_gpu_plugin_detector_path

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: CGroups Hierarchy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the CGroups Hierarchy parameter.

Related Name

Default Value

false

API Name

role_config_suppression_linux_container_executor_cgroups_hierarchy

Required

true

Suppress Parameter Validation: NodeManager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Healthchecker Script Arguments

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Healthchecker Script Arguments parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_healthchecker_script_args

Required

true

Suppress Parameter Validation: Healthchecker Script Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Healthchecker Script Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_healthchecker_script_path

Required

true

Suppress Parameter Validation: Java Configuration Options for NodeManager

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for NodeManager parameter.

Related Name

Default Value

false

API Name

role_config_suppression_node_manager_java_opts

Required

true

Suppress Parameter Validation: NodeManager Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_node_manager_log_dir

Required

true

Suppress Parameter Validation: NodeManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_config_safety_valve

Required

true

Suppress Parameter Validation: NodeManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_mapred_safety_valve

Required

true

Suppress Parameter Validation: NodeManager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_role_env_safety_valve

Required

true

Suppress Parameter Validation: NodeManager Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Web Application HTTPS Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_webserver_https_port

Required

true

Suppress Parameter Validation: NodeManager Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Web Application HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_webserver_port

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Allowed Devices for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Devices for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_devices

Required

true

Suppress Parameter Validation: Allowed Read-Only Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Read-Only Mounts for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_ro_mounts

Required

true

Suppress Parameter Validation: Allowed Read-Write Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Read-Write Mounts for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_rw_mounts

Required

true

Suppress Parameter Validation: Allowed Volume Drivers for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Volume Drivers for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_volume_drivers

Required

true

Suppress Parameter Validation: Docker Binary Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Docker Binary Path parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_binary

Required

true

Suppress Configuration Validator: Validates configuration of YARN NodeManagers when Docker on YARN feature is enabled.

Description

Whether to suppress configuration warnings produced by the Validates configuration of YARN NodeManagers when Docker on YARN feature is enabled. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_on_yarn_validator

Required

true

Suppress Parameter Validation: Trusted Registries for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Trusted Registries for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_trusted_registries

Required

true

Suppress Configuration Validator: YARN FPGA Resources Validator

Description

Whether to suppress configuration warnings produced by the YARN FPGA Resources Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_fpga_validator

Required

true

Suppress Configuration Validator: YARN GPU Resources Validator

Description

Whether to suppress configuration warnings produced by the YARN GPU Resources Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_gpu_validator

Required

true

Suppress Parameter Validation: NodeManager IPC Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager IPC Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_address

Required

true

Suppress Parameter Validation: Containers Environment Variable

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Containers Environment Variable parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_admin_env

Required

true

Suppress Parameter Validation: Containers Environment Variables Whitelist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Containers Environment Variables Whitelist parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_env_whitelist

Required

true

Suppress Parameter Validation: FPGA initializer script

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the FPGA initializer script parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_fpga_plugin_initializer_script

Required

true

Suppress Parameter Validation: NodeManager Local Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Local Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_local_dirs

Required

true

Suppress Parameter Validation: Localizer Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Localizer Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_localizer_address

Required

true

Suppress Parameter Validation: Minimum Hard Limit for Log Aggregation Roll Monitoring Interval

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Minimum Hard Limit for Log Aggregation Roll Monitoring Interval parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds_min

Required

true

Suppress Configuration Validator: Log Aggregation Roll Monitoring Interval Minimum Validator

Description

Whether to suppress configuration warnings produced by the Log Aggregation Roll Monitoring Interval Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds_minimum_validator

Required

true

Suppress Parameter Validation: NodeManager Container Log Directories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Container Log Directories parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_dirs

Required

true

Suppress Parameter Validation: NodeManager Recovery Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the NodeManager Recovery Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_recovery_dir

Required

true

Suppress Parameter Validation: Remote App Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_remote_app_log_dir

Required

true

Suppress Parameter Validation: Remote App Log Directory Suffix

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory Suffix parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_remote_app_log_dir_suffix

Required

true

Suppress Parameter Validation: Allowed FPGA devices

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed FPGA devices parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_allowed_fpga_devices

Required

true

Suppress Parameter Validation: List of available FPGA devices

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the List of available FPGA devices parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_available_devices

Required

true

Suppress Parameter Validation: Path to FPGA (aocl) tool

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to FPGA (aocl) tool parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_path_to_discovery_executables

Required

true

Suppress Parameter Validation: Allowed Linux Runtimes

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Linux Runtimes parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_allowed_runtimes

Required

true

Suppress Parameter Validation: Allowed Docker Container Networks

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Docker Container Networks parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_allowed_container_networks

Required

true

Suppress Parameter Validation: Docker Capabilities

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Docker Capabilities parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_capabilities

Required

true

Suppress Parameter Validation: Default Docker Container Network

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Docker Container Network parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_container_network

Required

true

Suppress Parameter Validation: Default Read-Only Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Read-Only Mounts for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_ro_mounts

Required

true

Suppress Parameter Validation: Default Read-Write Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Read-Write Mounts for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_rw_mounts

Required

true

Suppress Parameter Validation: Default Tempfs Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Tempfs Mounts for Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_tmpfs_mounts

Required

true

Suppress Parameter Validation: ACL for Privileged Docker Containers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ACL for Privileged Docker Containers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_privileged_containers_acl

Required

true

Suppress Configuration Validator: YARN Resource Types Validator

Description

Whether to suppress configuration warnings produced by the YARN Resource Types Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resources_validator

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_audit_health

Required

true

Suppress Health Test: ResourceManager Connectivity

Description

Whether to suppress the results of the ResourceManager Connectivity heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_connectivity

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_gc_duration

Required

true

Suppress Health Test: NodeManager Health Checker

Description

Whether to suppress the results of the NodeManager Health Checker heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_health_checker

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_node_manager_web_metric_collection

Required

true

Suppress Health Test: NodeManager Local Directories Free Space

Description

Whether to suppress the results of the NodeManager Local Directories Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nodemanager_local_data_directories_free_space

Required

true

Suppress Health Test: NodeManager Container Log Directories Free Space

Description

Whether to suppress the results of the NodeManager Container Log Directories Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nodemanager_log_directories_free_space

Required

true

Suppress Health Test: NodeManager Recovery Directory Free Space

Description

Whether to suppress the results of the NodeManager Recovery Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nodemanager_recovery_directory_free_space

Required

true

ResourceManager

Advanced

Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Advanced Configuration Snippet (Safety Valve) for Hadoop Metrics2. Properties will be inserted into hadoop-metrics2.properties.

Related Name

Default Value

API Name

hadoop_metrics2_safety_valve

Required

false

ResourceManager Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Java Configuration Options for ResourceManager

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

JAVA_GC_ARGS -Dlibrary.leveldbjni.path=CMF_CONF_DIR

API Name

resource_manager_java_opts

Required

false

ResourceManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only. A string to be inserted into yarn-site.xml for this role only.

Related Name

Default Value

API Name

resourcemanager_config_safety_valve

Required

false

ResourceManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only. A string to be inserted into mapred-site.xml for this role only.

Related Name

Default Value

API Name

resourcemanager_mapred_safety_valve

Required

false

ResourceManager Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

RESOURCEMANAGER_role_env_safety_valve

Required

false

ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_allow.txt

Description

For advanced use only. A string to be inserted into nodes_allow.txt for this role only.

Related Name

Default Value

API Name

rm_hosts_allow_safety_valve

Required

false

ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_exclude.txt

Description

For advanced use only. A string to be inserted into nodes_exclude.txt for this role only.

Related Name

Default Value

API Name

rm_hosts_exclude_safety_valve

Required

false

Logs

ResourceManager Logging Threshold

Description

The minimum log level for ResourceManager logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

ResourceManager Maximum Log File Backups

Description

The maximum number of rolled log files to keep for ResourceManager logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

ResourceManager Max Log Size

Description

The maximum size, in megabytes, per log file for ResourceManager logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

ResourceManager Log Directory

Description

Directory where ResourceManager will place its log files.

Related Name

hadoop.log.dir

Default Value

/var/log/hadoop-yarn

API Name

resource_manager_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

11130

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

startDelaySeconds: 10 ssl: false lowercaseOutputName: true lowercaseOutputLabelNames: true rules: - pattern: 'Hadoop<service=(.*), name=JvmMetrics><>(.*): (\d+)' attrNameSnakeCase: true name: $2 value: $3 labels: hadoop_service: $1 hadoop_metric_group: jvm_metrics

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

processors: filter/$ROLE_NAME: metrics: include: match_type: regexp metric_names: #memory - mem_heap_committed_m - mem_heap_max_m - mem_heap_used_m - mem_max_m - mem_non_heap_committed_m - mem_non_heap_used_m #gc - gc_.* #threads - threads_blocked - threads_new - threads_runnable - threads_terminated - threads_timed_waiting - threads_waiting #log - log_error - log_fatal - log_info - log_warn #process - process_cpu_seconds_total - process_start_time_seconds - process_open_fds - process_virtual_memory_bytes

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'DMP-$ROLE_NAME' scrape_interval: 60s scheme: 'http' static_configs: - targets: ['localhost:$ROLE_PARAM(jmx_exporter_port)'] labels: host: $HOST_NAME cm_cluster_id: $CLUSTER_ID service_type: $SERVICE_TYPE service_name: $SERVICE_NAME role_type: $ROLE_TYPE role_name: $ROLE_NAME node_instance_id: $INFRA(instance_id) resource_crn:

$INFRA(resource_crn) platform: $INFRA(platform) formfactor: paas-vm relabel_configs: - source_labels: [resource_crn] regex: 'crn:cdp:([^:]+):.*' replacement: '$$1' target_label: app_type action: replace

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] processors: [filter/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

resourcemanager_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

resourcemanager_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

resourcemanager_gc_duration_window

Required

false

ResourceManager Host Health Test

Description

When computing the overall ResourceManager health, consider the host's health.

Related Name

Default Value

true

API Name

resourcemanager_host_health_enabled

Required

false

ResourceManager Process Health Test

Description

Enables the health test that the ResourceManager's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

resourcemanager_scm_health_enabled

Required

false

Health Test Startup Tolerance

Description

The amount of time allowed after this role is started that failures of health tests that rely on communication with this role will be tolerated.

Related Name

Default Value

5 minute(s)

API Name

resourcemanager_startup_tolerance_minutes

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

resourcemanager_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

resourcemanager_web_metric_collection_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more

details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve)

Description

Enter an XML string that represents the Capacity Scheduler configuration.

Related Name

Default Value

<configuration> <property> <name>yarn.scheduler.capacity.root.queues</name> <value>default</value> </property> <property> <name>yarn.scheduler.capacity.root.capacity</name> <value>100</value> </property> <property> <name>yarn.scheduler.capacity.root.default.capacity</name> <value>100</value> </property> <property> <name>yarn.scheduler.capacity.root.default.maximum-am-resource-percent</

name> <value>0.2</value> </property> <property> <name>yarn.scheduler.capacity.schedule-asynchronously.enable</name> <value>true</value> </property> </configuration>

API Name

resourcemanager_capacity_scheduler_configuration

Required

true

Fair Scheduler Assign Multiple Tasks

Description

Enables multiple Fair Scheduler container assignments in one heartbeat, which improves cluster throughput when there are many small tasks to run.

Related Name

yarn.scheduler.fair.assignmultiple

Default Value

true

API Name

resourcemanager_fair_scheduler_assign_multiple

Required

true

Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

An XML string that will be inserted verbatim into the Fair Scheduler allocations file. For CDH 5, overrides the configuration set using the Pools configuration UI. For CDH 4, this is the only way to configure the Fair Scheduler for YARN.

Related Name

Default Value

API Name

resourcemanager_fair_scheduler_configuration

Required

false

Fair Scheduler Dynamic Max Assign

Description

During node heartbeat, the ResourceManager will allocate up to half the available resources on a node. Only valid if yarn.scheduler.fair.assignmultiple is set to true.

Related Name

yarn.scheduler.fair.dynamic.max.assign

Default Value

true

API Name

resourcemanager_fair_scheduler_dynamic_max_assign

Required

false

Fair Scheduler Max Assign

Description

Limit the number of containers allocated by the ResourceManager with each node heartbeat. -1 is equivalent to unlimited. Only valid if yarn.scheduler.fair.assignmultiple is true and yarn.scheduler.fair.dynamic.max.assign is false.

Related Name

yarn.scheduler.fair.max.assign

Default Value

-1

API Name

resourcemanager_fair_scheduler_max_assign

Required

false

Enable Fair Scheduler Preemption

Description

When enabled, if a pool's minimum share is not met for some period of time, the Fair Scheduler preempts applications in other pools. Preemption guarantees that production applications are not starved while also allowing the cluster to be used for experimental and research applications. To minimize wasted computation, the Fair Scheduler preempts the most recently launched applications.

Related Name

yarn.scheduler.fair.preemption

Default Value

false

API Name

resourcemanager_fair_scheduler_preemption

Required

true

Fair Scheduler Size-Based Weight

Description

When enabled, the Fair Scheduler will assign shares to individual apps based on their size, rather than providing an equal share to all apps regardless of size.

Related Name

yarn.scheduler.fair.sizebasedweight

Default Value

false

API Name

resourcemanager_fair_scheduler_size_based_weight

Required

true

Fair Scheduler User As Default Queue

Description

When set to true, the Fair Scheduler uses the username as the default pool name, in the event that a pool name is not specified. When set to false, all applications are run in a shared pool, called default.

Related Name

yarn.scheduler.fair.user-as-default-queue

Default Value

true

API Name

resourcemanager_fair_scheduler_user_as_default_queue

Required

true

ApplicationMaster Monitor Expiry

Description

The expiry interval to wait until an ApplicationMaster is considered dead.

Related Name

yarn.am.liveness-monitor.expiry-interval-ms

Default Value

10 minute(s)

API Name

yarn_am_liveness_monitor_expiry_interval_ms

Required

false

NodeManager Monitor Expiry

Description

The expiry interval to wait until a NodeManager is considered dead.

Related Name

yarn.nm.liveness-monitor.expiry-interval-ms

Default Value

10 minute(s)

API Name

yarn_nm_liveness_monitor_expiry_interval_ms

Required

false

Admin Client Thread Count

Description

Number of threads used to handle the ResourceManager admin interface.

Related Name

yarn.resourcemanager.admin.client.thread-count

Default Value

1

API Name

yarn_resourcemanager_admin_client_thread_count

Required

false

ApplicationMaster Maximum Attempts

Description

The maximum number of application attempts. This is a global setting for all ApplicationMasters.. Each ApplicationMaster can specify its individual maximum through the API, but if the individual maximum is more than the global maximum, the ResourceManager overrides it.

Related Name

yarn.resourcemanager.am.max-attempts

Default Value

2

API Name

yarn_resourcemanager_am_max_retries

Required

false

ApplicationMaster Monitor Interval

Description

The periodic interval that the ResourceManager will check whether ApplicationMasters is still alive.

Related Name

yarn.resourcemanager.amliveliness-monitor.interval-ms

Default Value

1 second(s)

API Name

yarn_resourcemanager_amliveliness_monitor_interval_ms

Required

false

Client Thread Count

Description

The number of threads used to handle applications manager requests.

Related Name

yarn.resourcemanager.client.thread-count

Default Value

50

API Name

yarn_resourcemanager_client_thread_count

Required

false

Container Monitor Interval

Description

The periodic interval that the ResourceManager will check whether containers are still alive.

Related Name

yarn.resourcemanager.container.liveness-monitor.interval-ms

Default Value

10 minute(s)

API Name

yarn_resourcemanager_container_liveness_monitor_interval_ms

Required

false

Max Completed Applications

Description

The maximum number of completed applications that the ResourceManager keeps.

Related Name

yarn.resourcemanager.max-completed-applications

Default Value

10000

API Name

yarn_resourcemanager_max_completed_applications

Required

false

NodeManager Monitor Interval

Description

The periodic interval that the ResourceManager will check whether NodeManagers are still alive.

Related Name

yarn.resourcemanager.nm.liveness-monitor.interval-ms

Default Value

1 second(s)

API Name

yarn_resourcemanager_nm_liveness_monitor_interval_ms

Required

false

Enable ResourceManager Proxy User Privileges

Description

When enabled, ResourceManager has proxy user privileges.

Related Name

yarn.resourcemanager.proxy-user-privileges.enabled

Default Value

true

API Name

yarn_resourcemanager_proxy_user_privileges_enabled

Required

false

Enable ResourceManager Recovery

Description

When enabled, any applications that were running on the cluster when the ResourceManager died will be recovered when the ResourceManager next starts. Note: If RM-HA is enabled, then this configuration is always enabled.

Related Name

yarn.resourcemanager.recovery.enabled

Default Value

true

API Name

yarn_resourcemanager_recovery_enabled

Required

false

Resource Tracker Thread Count

Description

Number of threads to handle resource tracker calls.

Related Name

yarn.resourcemanager.resource-tracker.client.thread-count

Default Value

50

API Name

yarn_resourcemanager_resource_tracker_client_thread_count

Required

false

Scheduler Thread Count

Description

The number of threads used to handle requests through the scheduler interface.

Related Name

yarn.resourcemanager.scheduler.client.thread-count

Default Value

50

API Name

yarn_resourcemanager_scheduler_client_thread_count

Required

false

ZooKeeper Session Timeout

Description

The timeout for the ResourceManager session with ZooKeeper. The session expires if the ZooKeeper ensemble does not hear from the ResourceManager within the specified timeout period (no heartbeat). Session expiration is managed by the ZooKeeper ensemble, not by the ResourceManager.

Related Name

yarn.resourcemanager.zk-timeout-ms

Default Value

1 minute(s)

API Name

yarn_resourcemanager_zk_timeout_ms

Required

false

Resource Calculator Class

Description

The Resource Calculator implementation to be used to compare Resources in the scheduler. The DefaultResourceCalculator only uses Memory while DominantResourceCalculator uses Dominant-resource to compare multi-dimensional resources such as Memory, CPU etc.

Related Name

yarn.scheduler.capacity.resource-calculator

Default Value

org.apache.hadoop.yarn.util.resource.DominantResourceCalculator

API Name

yarn_scheduler_capacity_resource_calculator

Required

false

Fair Scheduler Preemption Utilization Threshold

Description

The utilization threshold after which preemption kicks in. The utilization is computed as the maximum ratio of usage to capacity among all resources.

Related Name

yarn.scheduler.fair.preemption.cluster-utilization-threshold

Default Value

0.8

API Name

yarn_scheduler_fair_preemption_cluster_utilization_threshold

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

ResourceManager Web Application HTTPS Port (TLS/SSL)

Description

The HTTPS port of the ResourceManager web application.

Related Name

yarn.resourcemanager.webapp.https.address

Default Value

8090

API Name

resourcemanager_webserver_https_port

Required

false

ResourceManager Web Application HTTP Port

Description

The HTTP port of the ResourceManager web application.

Related Name

yarn.resourcemanager.webapp.address

Default Value

8088

API Name

resourcemanager_webserver_port

Required

false

ResourceManager Address

Description

The address of the applications manager interface in the ResourceManager.

Related Name

yarn.resourcemanager.address

Default Value

8032

API Name

yarn_resourcemanager_address

Required

false

Administration Address

Description

The address of the admin interface in the ResourceManager.

Related Name

yarn.resourcemanager.admin.address

Default Value

8033

API Name

yarn_resourcemanager_admin_address

Required

false

Resource Tracker Address

Description

The address of the resource tracker interface in the ResourceManager.

Related Name

yarn.resourcemanager.resource-tracker.address

Default Value

8031

API Name

yarn_resourcemanager_resource_tracker_address

Required

false

Scheduler Address

Description

The address of the scheduler interface in the ResourceManager.

Related Name

yarn.resourcemanager.scheduler.address

Default Value

8030

API Name

yarn_resourcemanager_scheduler_address

Required

false

Bind ResourceManager to Wildcard Address

Description

If enabled, the ResourceManager binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

yarn_rm_bind_wildcard

Required

false

Resource Management

Java Heap Size of ResourceManager in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

resource_manager_java_heapsize

Required

false

Fair Scheduler Node Locality Threshold

Description

For applications that request containers on particular nodes, the number of scheduling opportunities since the last container assignment to wait before accepting a placement on another node. Expressed as a float between 0 and 1, which, as a fraction of the cluster size, is the number of scheduling opportunities to pass up. If not set, this means don't pass up any scheduling opportunities.
Requires Fair Scheduler continuous scheduling to be disabled. If continuous scheduling is enabled, yarn.scheduler.fair.locality-delay-node-ms should be used instead.

Related Name

yarn.scheduler.fair.locality.threshold.node

Default Value

API Name

resourcemanager_fair_scheduler_locality_threshold_node

Required

false

Fair Scheduler Rack Locality Threshold

Description

For applications that request containers on particular racks, the number of scheduling opportunities since the last container assignment to wait before accepting a placement on another rack. Expressed as a float between 0 and 1, which, as a fraction of the cluster size, is the number of scheduling opportunities to pass up. If not set, this means don't pass up any scheduling opportunities.
Requires Fair Scheduler continuous scheduling to be disabled. If continuous scheduling is enabled, yarn.scheduler.fair.locality-delay-rack-ms should be used instead.

Related Name

yarn.scheduler.fair.locality.threshold.rack

Default Value

API Name

resourcemanager_fair_scheduler_locality_threshold_rack

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Enable Fair Scheduler Continuous Scheduling

Description

Enable continuous scheduling in the Fair Scheduler. When enabled, scheduling decisions are decoupled from NodeManager heartbeats, leading to faster resource allocations.

Related Name

yarn.scheduler.fair.continuous-scheduling-enabled

Default Value

false

API Name

yarn_scheduler_fair_continuous_scheduling_enabled

Required

false

Fair Scheduler Node Locality Delay

Description

For applications that request containers on particular nodes, the minimum time in milliseconds the Fair Scheduler waits before accepting a placement on another node. Requires Fair Scheduler continuous scheduling to be enabled. If continuous scheduling is disabled, yarn.scheduler.fair.locality.threshold.node should be used instead.

Related Name

yarn.scheduler.fair.locality-delay-node-ms

Default Value

2 second(s)

API Name

yarn_scheduler_fair_locality_delay_node_ms

Required

false

Fair Scheduler Rack Locality Delay

Description

For applications that request containers on particular racks, the minimum time in milliseconds the Fair Scheduler waits before accepting a placement on another rack. Requires Fair Scheduler continuous scheduling to be enabled. If continuous scheduling is disabled, yarn.scheduler.fair.locality.threshold.rack should be used instead.

Related Name

yarn.scheduler.fair.locality-delay-rack-ms

Default Value

4 second(s)

API Name

yarn_scheduler_fair_locality_delay_rack_ms

Required

false

Container Memory Increment

Description

If using the Fair Scheduler, memory requests will be rounded up to the nearest multiple of this number. This parameter has no effect prior to CDH 5.

Related Name

yarn.scheduler.increment-allocation-mb

Default Value

512 MiB

API Name

yarn_scheduler_increment_allocation_mb

Required

true

Container Virtual CPU Cores Increment

Description

If using the Fair Scheduler, virtual core requests will be rounded up to the nearest multiple of this number. This parameter has no effect prior to CDH 5.

Related Name

yarn.scheduler.increment-allocation-vcores

Default Value

1

API Name

yarn_scheduler_increment_allocation_vcores

Required

true

Container Memory Maximum

Description

The largest amount of physical memory, in MiB, that can be requested for a container.

Related Name

yarn.scheduler.maximum-allocation-mb

Default Value

64 GiB

API Name

yarn_scheduler_maximum_allocation_mb

Required

true

Container Virtual CPU Cores Maximum

Description

The largest number of virtual CPU cores that can be requested for a container. This parameter has no effect prior to CDH 4.4.

Related Name

yarn.scheduler.maximum-allocation-vcores

Default Value

32

API Name

yarn_scheduler_maximum_allocation_vcores

Required

true

Container Memory Minimum

Description

The smallest amount of physical memory, in MiB, that can be requested for a container. If using the Capacity or FIFO scheduler (or any scheduler, prior to CDH 5), memory requests will be rounded up to the nearest multiple of this number.

Related Name

yarn.scheduler.minimum-allocation-mb

Default Value

1 GiB

API Name

yarn_scheduler_minimum_allocation_mb

Required

true

Container Virtual CPU Cores Minimum

Description

The smallest number of virtual CPU cores that can be requested for a container. If using the Capacity or FIFO scheduler (or any scheduler, prior to CDH 5), virtual core requests will be rounded up to the nearest multiple of this number. This parameter has no effect prior to CDH 4.4.

Related Name

yarn.scheduler.minimum-allocation-vcores

Default Value

1

API Name

yarn_scheduler_minimum_allocation_vcores

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: ResourceManager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Java Configuration Options for ResourceManager

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for ResourceManager parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resource_manager_java_opts

Required

true

Suppress Parameter Validation: ResourceManager Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resource_manager_log_dir

Required

true

Suppress Parameter Validation: Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_capacity_scheduler_configuration

Required

true

Suppress Parameter Validation: ResourceManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_config_safety_valve

Required

true

Suppress Parameter Validation: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_fair_scheduler_configuration

Required

true

Suppress Parameter Validation: ResourceManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_mapred_safety_valve

Required

true

Suppress Parameter Validation: ResourceManager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_role_env_safety_valve

Required

true

Suppress Parameter Validation: ResourceManager Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Web Application HTTPS Port (TLS/SSL) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_webserver_https_port

Required

true

Suppress Parameter Validation: ResourceManager Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Web Application HTTP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_webserver_port

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_allow.txt

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_allow.txt parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_hosts_allow_safety_valve

Required

true

Suppress Parameter Validation: ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_exclude.txt

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_exclude.txt parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_hosts_exclude_safety_valve

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: ResourceManager Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ResourceManager Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_address

Required

true

Suppress Parameter Validation: Administration Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Administration Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_admin_address

Required

true

Suppress Parameter Validation: ApplicationMaster Maximum Attempts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ApplicationMaster Maximum Attempts parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_am_max_retries

Required

true

Suppress Parameter Validation: Resource Tracker Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Resource Tracker Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_resource_tracker_address

Required

true

Suppress Parameter Validation: Scheduler Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Scheduler Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_scheduler_address

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_otelcol_health

Required

true

Suppress Health Test: Ranger Plugin Hdfs Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Hdfs Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_ranger_plugin_hdfs_spool_directory_size_health

Required

true

Suppress Health Test: Ranger Plugin Solr Spool Directory Size

Description

Whether to suppress the results of the Ranger Plugin Solr Spool Directory Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_ranger_plugin_solr_spool_directory_size_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_resource_manager_web_metric_collection

Required

true

Service-Wide

Advanced

System User's Home Directory

Description

The home directory of the system user on the local filesystem. This setting must reflect the system's configured value - only changing it here will not change the actual home directory.

Related Name

Default Value

/var/lib/hadoop-yarn

API Name

hdfs_user_home_dir

Required

true

HDFS Replication Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

For advanced use only, a string to be inserted into mapred-site.xml. Applies to all HDFS Replication jobs.

Related Name

Default Value

API Name

mapreduce_service_replication_config_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as. (Except the Job History Server, which has its own group.)

Related Name

Default Value

hadoop

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as. (Except the Job History Server, which has its own user)

Related Name

Default Value

yarn

API Name

process_username

Required

true

YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-audit.xml

Description

For advanced use only, a string to be inserted into ranger-yarn-audit.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_audit_safety_valve

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-policymgr-ssl.xml

Description

For advanced use only, a string to be inserted into ranger-yarn-policymgr-ssl.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_policymgr_ssl_safety_valve

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-security.xml

Description

For advanced use only, a string to be inserted into ranger-yarn-security.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ranger_security_safety_valve

Required

false

YARN Application Classpath

Description

Entries to add to the classpaths of YARN applications.

Related Name

yarn.application.classpath

Default Value

$HADOOP_CLIENT_CONF_DIR $HADOOP_COMMON_HOME/* $HADOOP_COMMON_HOME/lib/* $HADOOP_HDFS_HOME/* $HADOOP_HDFS_HOME/lib/* $HADOOP_YARN_HOME/* $HADOOP_YARN_HOME/lib/*

API Name

yarn_application_classpath

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

For advanced use only, a string to be inserted into core-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_core_site_safety_valve

Required

false

Fair Scheduler Configuration Rules (Deployed)

Description

A list specifying the rules to run to determine which Fair Scheduler configuration to use.

Related Name

Default Value

[]

API Name

yarn_fs_schedule_rules

Required

false

Fair Scheduler Configuration Rules (Staged)

Description

A list specifying the rules to run to determine which Fair Scheduler configuration to use. Typically edited using the Rules configuration UI.

Related Name

Default Value

API Name

yarn_fs_schedule_rules_draft

Required

false

Fair Scheduler Allocations (Deployed)

Description

JSON representation of all the configurations that the Fair Scheduler can take on across all schedules.

Related Name

Default Value

queuePlacementRules: [create: true, name: specified , name: nestedUserQueue, rules: [name: default, queue: users]], queues: [name: root, queues: [name: default, queues: [], schedulablePropertiesList: [scheduleName: default], schedulingPolicy: drf , name: users, queues: [], schedulablePropertiesList: [scheduleName: default], schedulingPolicy: drf, type: parent], schedulablePropertiesList: [scheduleName: default], schedulingPolicy: drf], users: []

API Name

yarn_fs_scheduled_allocations

Required

false

Fair Scheduler Allocations (Staged)

Description

JSON representation of all the configurations that the Fair Scheduler can take on across all schedules. Typically edited using the Pools configuration UI.

Related Name

Default Value

API Name

yarn_fs_scheduled_allocations_draft

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml

Description

For advanced use only, a string to be inserted into hadoop-policy.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_hadoop_policy_config_safety_valve

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only, a string to be inserted into yarn-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_service_config_safety_valve

Required

false

YARN Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_service_env_safety_valve

Required

false

YARN Service MapReduce Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into mapred-site.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_service_mapred_safety_valve

Required

false

HDFS Replication Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

For advanced use only, a string to be inserted into yarn-site.xml. Applies to all HDFS Replication jobs.

Related Name

Default Value

API Name

yarn_service_replication_config_safety_valve

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

For advanced use only, a string to be inserted into ssl-client.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_ssl_client_safety_valve

Required

false

YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

For advanced use only, a string to be inserted into ssl-server.xml. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

yarn_ssl_server_safety_valve

Required

false

Log Aggregation

Enable Log Aggregation

Description

Specifies if log aggregation is enabled.

Related Name

yarn.log-aggregation-enable

Default Value

true

API Name

yarn_log_aggregation_enable

Required

false

Supported Log Aggregation File Formats

Description

Specifies which log file formats are supported. The first file format in the list is used to write the aggregated logs. TFile format is always added to support backward compatibility.

Related Name

yarn.log-aggregation.file-formats

Default Value

IFile TFile

API Name

yarn_log_aggregation_file_formats

Required

false

Remote App Log Directory for IFile Format

Description

Specifies the path of the directory where application logs are stored after an application is completed if IFile format is given as the file format for writing. This configuration overwrites the one given in NodeManager level (yarn.nodemanager.remote-app-log-dir).

Related Name

yarn.log-aggregation.IFile.remote-app-log-dir

Default Value

API Name

yarn_log_aggregation_IFile_remote_app_log_dir

Required

false

Remote App Log Directory Suffix for IFile Format

Description

The remote log directory is created at {remote-app-log-dir}/${user}/{thisParam} if IFile format is selected for writing. This configuration overwrites the one given in NodeManager level (yarn.nodemanager.remote-app-log-dir-suffix).

Related Name

yarn.log-aggregation.IFile.remote-app-log-dir-suffix

Default Value

API Name

yarn_log_aggregation_IFile_remote_app_log_dir_suffix

Required

false

Log Aggregation Retention Period

Description

Specifies how long aggregation logs are kept before they are deleted.

Related Name

yarn.log-aggregation.retain-seconds

Default Value

7 day(s)

API Name

yarn_log_aggregation_retain_seconds

Required

false

Log Aggregation Status Timeout

Description

Specifies the maximum amount of time that the NodeManager has for reporting a container's log aggregation status. If no log aggregation status is sent by the NodeManager within the allotted time, the ResourceManager reports a TIME_OUT log aggregation status for that container.

Related Name

yarn.log-aggregation-status.time-out.ms

Default Value

10 minute(s)

API Name

yarn_log_aggregation_status_time_out_ms

Required

false

Remote App Log Directory for TFile Format

Description

Specifies the path of the directory where application logs are stored after an application is completed if TFile format is selected for writing. This configuration overwrites the one given in NodeManager level (yarn.nodemanager.remote-app-log-dir).

Related Name

yarn.log-aggregation.TFile.remote-app-log-dir

Default Value

API Name

yarn_log_aggregation_TFile_remote_app_log_dir

Required

false

Remote App Log Directory Suffix for TFile Format

Description

The remote log directory is created at {remote-app-log-dir}/${user}/{thisParam} if TFile format is selected for writing. This configuration overwrites the one given in NodeManager level (yarn.nodemanager.remote-app-log-dir-suffix).

Related Name

yarn.log-aggregation.TFile.remote-app-log-dir-suffix

Default Value

API Name

yarn_log_aggregation_TFile_remote_app_log_dir_suffix

Required

false

Log Aggregation Compression Type

Description

Specifies the TFile compression type used to compress aggregated logs.

Related Name

yarn.nodemanager.log-aggregation.compression-type

Default Value

none

API Name

yarn_nodemanager_log_aggregation_compression_type

Required

false

Monitoring

Admin Users Applications List Visibility Settings

Description

Controls which applications an admin user can see in the applications list view

Related Name

Default Value

ALL

API Name

admin_application_list_settings

Required

true

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Cloudera Manager Container Usage Metrics Directory

Description

DFS directory where the container usage metrics from Cloudera Manager sink are stored by YARN NodeManagers. Cloudera Service Monitor will read the container usage metrics and aggregate them for generating usage reports. Note: If you change this, you will need to re-run the Create YARN Container Usage Metrics Dir command.

Related Name

Default Value

/tmp/cmYarnContainerMetrics

API Name

cm_yarn_container_usage_input_dir

Required

true

Maximum Hours to Aggregate Usage Metrics

Description

Maximum number of hours in the past for which container usage aggregation is performed by Cloudera Service Monitor.

Related Name

Default Value

6

API Name

cm_yarn_container_usage_job_go_back_window_hours

Required

true

Reduce Tasks for Container Usage MapReduce Job

Description

Number of reduce tasks to use for the MapReduce job to aggregate container usage metrics.

Related Name

Default Value

1

API Name

cm_yarn_container_usage_job_num_reduce_tasks

Required

true

Container Usage MapReduce Job Pool

Description

YARN pool which is used to submit the job to aggregate container usage metrics.

Related Name

Default Value

API Name

cm_yarn_container_usage_job_pool

Required

false

Container Usage MapReduce Job User

Description

User that Cloudera Service Monitor uses to run the MapReduce job to aggregate container usage metrics. Note: If you change this user, you need to change the owner of the existing Container Usage Metrics and Output Directories.

Related Name

Default Value

API Name

cm_yarn_container_usage_job_user

Required

false

Container Usage Output Directory

Description

DFS directory where the aggregated container usage metrics are stored by Cloudera Service Monitor. This directory is created by Cloudera Service Monitor before running the usage aggregation MapReduce job for the first time.

Related Name

Default Value

/tmp/cmYarnContainerMetricsAggregate

API Name

cm_yarn_container_usage_output_dir

Required

true

Enable Container Usage Metrics Collection

Description

Enables storing YARN container usage metrics in HDFS and periodically running a MapReduce job from Cloudera Service Monitor to aggregate them into per-application metrics. This is required for YARN usage reporting to work.

Related Name

Default Value

false

API Name

cm_yarn_enable_container_usage_aggregation

Required

true

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Event Retry Frequency

Description

The frequency in which the log4j event publication appender will retry sending undelivered log events to the Event server, in seconds

Related Name

Default Value

30

API Name

log_event_retry_frequency

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Client Config Overrides

Description

For advanced use only, a list of configuration properties that will be used by the Service Monitor instead of the current client configuration for the service.

Related Name

Default Value

<property> <name>mapreduce.output.fileoutputformat.compress</name> <value>false</value> </property> <property> <name>mapreduce.output.fileoutputformat.compress.codec</name> <value>org.apache.hadoop.io.compress.DefaultCodec</value> </property> <property> <name>io.compression.codecs</name> <value>org.apache.hadoop.io.compress.DefaultCodec, org.apache.hadoop.io.compress.GzipCodec, org.apache.hadoop.io.compress.BZip2Codec, org.apache.hadoop.io.compress.DeflateCodec, org.apache.hadoop.io.compress.SnappyCodec, org.apache.hadoop.io.compress.Lz4Codec</value> </property>

API Name

smon_client_config_overrides

Required

false

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Non-Admin Users Applications List Visibility Settings

Description

Controls which applications non-admin users can see in the applications list view

Related Name

Default Value

ALL

API Name

user_application_list_settings

Required

true

Active ResourceManager Detection Window

Description

The tolerance window used in YARN service tests that depend on detection of the active ResourceManager.

Related Name

Default Value

3 minute(s)

API Name

yarn_active_resourcemanager_detection_window

Required

false

YARN Application Aggregates

Description

Controls the aggregate metrics generated for YARN applications. The structure is a JSON list of the attributes to aggregate and the entities to aggregate to. For example, if the attributeName is 'maps_completed' and the aggregationTargets is ['USER'] then the Service Monitor will create the metric 'yarn_application_maps_completed_rate' and, every ten minutes, will record the total maps completed for each user across all their YARN applications. By default it will also record the number of applications submitted ('apps_submitted_rate') for both users and pool. For a full list of the supported attributes see the YARN search page. Note that the valid aggregation targets are USER, YARN_POOL, and YARN (the service), and that these aggregate metrics can be viewed on both the reports and charts search pages.

Related Name

Default Value

[attributeName: maps_total, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: reduces_total, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: cpu_milliseconds, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: mb_millis_maps, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: mb_millis_reduces, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: vcores_millis_maps, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: vcores_millis_reduces, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: file_bytes_read, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: file_bytes_written, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: hdfs_bytes_read, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: hdfs_bytes_written, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: cm_cpu_milliseconds, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: application_duration, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: s3a_bytes_read, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: s3a_bytes_written, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: adl_bytes_read, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER] , attributeName: adl_bytes_written, aggregationTargets: [USER, YARN_POOL_USER, YARN_POOL, YARN, CLUSTER]]

API Name

yarn_application_aggregates

Required

false

Container Metrics Sampling Interval

Description

Interval at which YARN container usage metrics are sampled. Increasing this configuration can reduce the accuracy of container usage metrics, whereas setting it too low will increase the resources used to compute container usage.

Related Name

yarn.nodemanager.container-monitor.interval-ms

Default Value

3 second(s)

API Name

yarn_container_seconds_per_sample

Required

true

JobHistory Server Role Health Test

Description

When computing the overall YARN health, consider JobHistory Server's health

Related Name

Default Value

true

API Name

yarn_jobhistoryserver_health_enabled

Required

false

Healthy NodeManager Monitoring Thresholds

Description

The health test thresholds of the overall NodeManager health. The check returns "Concerning" health if the percentage of "Healthy" NodeManagers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" NodeManagers falls below the critical threshold.

Related Name

Default Value

Warning: 95.0 %, Critical: 90.0 %

API Name

yarn_nodemanagers_healthy_thresholds

Required

false

ResourceManager Activation Startup Tolerance

Description

The amount of time after ResourceManager(s) start that the lack of an active ResourceManager will be tolerated. This is an advanced option that does not often need to be changed.

Related Name

Default Value

3 minute(s)

API Name

yarn_resourcemanager_activation_startup_tolerance

Required

false

Active ResourceManager Role Health Check

Description

When computing the overall YARN service health, whether to consider the active ResourceManager's health.

Related Name

Default Value

true

API Name

yarn_resourcemanagers_health_enabled

Required

false

Standby ResourceManager Health Check

Description

When computing the overall YARN service health, whether to consider the health of the standby ResourceManager.

Related Name

Default Value

true

API Name

yarn_standby_resourcemanager_health_enabled

Required

false

Other

HDFS Service

Description

Name of the HDFS service that this YARN service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Serve logs over HTTP

Description

Whether to serve logs over HTTP from YARN web servers. This includes listing the logs directory at the /logs endpoint, which may be a security concern.

Related Name

hadoop.http.logs.enabled

Default Value

true

API Name

http_logs_enabled

Required

false

SSL Encryption for MapReduce Shuffle

Description

Specifies if encrypted shuffle is enabled.

Related Name

mapreduce.shuffle.ssl.enabled

Default Value

false

API Name

mapreduce_shuffle_ssl_enabled

Required

false

Queue Manager Service

Description

Name of the Queue Manager service that this YARN service instance depends on

Related Name

Default Value

API Name

queuemanager_service

Required

false

Ranger Plugin Enable YARN ACLs Fallback

Description

By default, fallback is enabled for YARN, which mean if the access cannot be determined by Ranger policies, authorization will fallback to YARN ACLs. If this behavior needs to be changed, you can disable the config.

Related Name

ranger.add-yarn-authorization

Default Value

true

API Name

ranger_plugin_enable_fallback_authorization

Required

false

Ranger Plugin Trusted Proxy IP Address

Description

Accepts a list of IP addresses of proxy servers for trusting.

Related Name

ranger.plugin.yarn.trusted.proxy.ipaddress

Default Value

API Name

ranger_plugin_trusted_proxy_ipaddress

Required

false

Ranger Plugin Use X-Forwarded for IP Address

Description

The parameter is used for identifying the originating IP address of a user connecting to a component through proxy for audit logs.

Related Name

ranger.plugin.yarn.use.x-forwarded-for.ipaddress

Default Value

false

API Name

ranger_plugin_use_x_forwarded_for_ipaddress

Required

false

Ranger Service

Description

Name of the Ranger service that this Yarn service instance depends on

Related Name

Default Value

API Name

ranger_service

Required

false

Enable ResourceManager ACLs

Description

Whether users and groups specified in Admin ACL should be checked for authorization to perform admin operations.

Related Name

yarn.acl.enable

Default Value

true

API Name

yarn_acl_enable

Required

false

Admin ACL

Description

ACL that determines which users and groups can submit and kill applications in any pool, and can issue commands on ResourceManager roles.

Related Name

yarn.admin.acl

Default Value

API Name

yarn_admin_acl

Required

false

Node Labels

Description

Enable YARN Node Labels.

Related Name

yarn.node-labels.enabled

Default Value

true

API Name

yarn_node_labels_enabled

Required

false

Capacity Scheduler Auto Queue Deletion

Description

Enables auto created queue deletion for ResourceManager Capacity Scheduler.

Related Name

yarn_resourcemanager_capacity_scheduler_aqc_auto_deletion

Default Value

true

API Name

yarn_resourcemanager_capacity_scheduler_aqc_auto_deletion

Required

false

Capacity Scheduler Preemption

Description

Enables Preemption for ResourceManager Capacity Scheduler.

Related Name

yarn_resourcemanager_capacity_scheduler_preemption

Default Value

true

API Name

yarn_resourcemanager_capacity_scheduler_preemption

Required

false

Node Manager Graceful Decommission Timeout

Description

This is the maximum time to wait for running containers and applications to complete before transition a DECOMMISSIONING node into DECOMMISSIONED. (-1 indicates infinite timeout, 0 indicates non-graceful)

Related Name

yarn.resourcemanager.nodemanager-graceful-decommission-timeout-secs

Default Value

0 second(s)

API Name

yarn_resourcemanager_nodemanager_graceful_decommission_timeout_secs

Required

false

RM-HA Cluster ID

Description

Cluster ID used when ResourceManager is Highly Available.

Related Name

yarn.resourcemanager.cluster-id

Default Value

yarnRM

API Name

yarn_rm_ha_cluster_id

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this YARN service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

false

Proxy

Llama Proxy User Groups

Description

Comma-delimited list of groups that you want to allow the Llama (AM for Impala) user to impersonate. The default '*' allows all groups. To disable entirely, use a string that doesn't correspond to a group name, such as '_no_group_'.

Related Name

hadoop.proxyuser.llama.groups

Default Value

*

API Name

llama_proxy_user_groups_list

Required

false

Llama Proxy User Hosts

Description

Comma-delimited list of hosts where you want to allow the Llama (AM for Impala) user to impersonate other users. The default '*' allows all hosts. To disable entirely, use a string that doesn't correspond to a host name, such as '_no_host'.

Related Name

hadoop.proxyuser.llama.hosts

Default Value

*

API Name

llama_proxy_user_hosts_list

Required

false

Resource Management

Limit Nonsecure Container Executor Users

Description

This determines the user Linux container executor should run as on a non-secure cluster.
If this value is set to true, then all containers will be launched as the user specified in yarn.nodemanager.linux-container-executor.nonsecure-mode.local-user. If this value is set to false, then containers will run as the user who submitted the application.

Related Name

Default Value

true

API Name

yarn_nodemanager_linux_container_executor_nonsecure_mode_limit_users

Required

false

UNIX User for Nonsecure Mode with Linux Container Executor

Description

UNIX user that containers run as when Linux-container-executor is used in nonsecure mode.

Related Name

yarn.nodemanager.linux-container-executor.nonsecure-mode.local-user

Default Value

nobody

API Name

yarn_nodemanager_linux_container_executor_nonsecure_mode_local_user

Required

false

Allow Undeclared Pools

Description

When set to true, pools specified in applications but not explicitly configured, are created at runtime with default settings. When set to false, applications specifying pools not explicitly configured run in a pool named default. This setting applies when an application explicitly specifies a pool and when the application runs in a pool named with the username associated with the application.

Related Name

yarn.scheduler.fair.allow-undeclared-pools

Default Value

true

API Name

yarn_scheduler_fair_allow_undeclared_pools

Required

false

Use CGroups for Resource Management

Description

Whether YARN creates a cgroup per container, thereby isolating the CPU usage of containers. When set, yarn.nodemanager.linux-container-executor.resources-handler.class is configured to org.apache.hadoop.yarn.server.nodemanager.util.CgroupsLCEResourcesHandler. The host (in Cloudera Manager) must have cgroups enabled. The number of shares allocated to all YARN containers is configured by adjusting the CPU shares value of the Node Manager in the Resource Management configuration group.

Related Name

yarn.nodemanager.linux-container-executor.resources-handler.class

Default Value

false

API Name

yarn_service_cgroups

Required

false

Always Use Linux Container Executor

Description

Whether YARN uses the Linux Container Executor both in secure (Kerberos) and insecure (not Kerberos) environments. Cgroups enforcement only works when the Linux Container Executor is used.

Related Name

yarn.nodemanager.container-executor.class

Default Value

false

API Name

yarn_service_lce_always

Required

false

Resource Types

Resource Types

Description

Resource definition can be extended to include arbitrary countable resources. A countable resource is a resource that is consumed while a container is running, but is released afterwards. CPU, memory and GPU are countable resources.

Related Name

Default Value

API Name

resource_types

Required

false

Security

Enable Kerberos Authentication for HTTP Web-Consoles

Description

Enables Kerberos authentication for Hadoop HTTP web consoles for all roles of this service using the SPNEGO protocol. Note: This is effective only if Kerberos is enabled.

Related Name

Default Value

false

API Name

hadoop_secure_web_ui

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

yarn

API Name

kerberos_princ_name

Required

true

Hive LLAP Kerberos Conf Staging Path

Description

Staging directory for Hive LLAP Kerberos Configuration. This should generally not be changed.

Related Name

hive_llap_kerberos_staging_path

Default Value

/var/lib/hadoop-yarn

API Name

llap_kerberos_staging_path

Required

false

Ranger DFS Audit Path

Description

The DFS path on which Ranger audits are written. The special placeholder '${ranger_base_audit_url}' should be used as the prefix, in order to use the centralized location defined in the Ranger service.

Related Name

xasecure.audit.destination.hdfs.dir

Default Value

$ranger_base_audit_url/yarn

API Name

ranger_audit_hdfs_dir

Required

false

Ranger Audit DFS Spool Dir

Description

Spool directory for Ranger audits being written to DFS.

Related Name

xasecure.audit.destination.hdfs.batch.filespool.dir

Default Value

/var/log/yarn/audit/hdfs/spool

API Name

ranger_audit_hdfs_spool_dir

Required

false

Ranger Audit Solr Spool Dir

Description

Spool directory for Ranger audits being written to Solr.

Related Name

xasecure.audit.destination.solr.batch.filespool.dir

Default Value

/var/log/yarn/audit/solr/spool

API Name

ranger_audit_solr_spool_dir

Required

false

Ranger Policy Cache Directory

Description

The directory where Ranger security policies are cached locally.

Related Name

ranger.plugin.yarn.policy.cache.dir

Default Value

/var/lib/ranger/yarn/policy-cache

API Name

ranger_policy_cache_dir

Required

false

TLS/SSL Client Truststore File Location

Description

Path to the truststore file used when roles of this service act as TLS/SSL clients. Overrides the cluster-wide default truststore location set in Core Configuration. This truststore must be in JKS format. The truststore contains certificates of trusted servers, or of Certificate Authorities trusted to identify servers. The contents of the truststore can be modified without restarting any roles. By default, changes to its contents are picked up within ten seconds. If not set, the default Java truststore is used to verify certificates.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

TLS/SSL Client Truststore File Password

Description

Password for the TLS/SSL client truststore. Overrides the cluster-wide default truststore password set in Core Configuration.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Hadoop TLS/SSL Server Keystore Key Password

Description

Password that protects the private key contained in the server keystore used for encrypted shuffle and encrypted web UIs. Applies to all configurations of daemon roles of this service.

Related Name

ssl.server.keystore.keypassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Hadoop TLS/SSL Server Keystore File Location

Description

Path to the keystore file containing the server certificate and private key used for encrypted shuffle and encrypted web UIs. Applies to configurations of all daemon roles of this service.

Related Name

ssl.server.keystore.location

Default Value

API Name

ssl_server_keystore_location

Required

false

Hadoop TLS/SSL Server Keystore File Password

Description

Password for the server keystore file used for encrypted shuffle and encrypted web UIs. Applies to configurations of all daemon roles of this service.

Related Name

ssl.server.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

SSL/TLS Cipher Suite

Description

The SSL/TLS cipher suites to use. "Modern 2018" is a modern set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. These cipher suites use strong

cryptography and are preferred unless interaction with older clients is required. These modern cipher suites are compatible with Firefox 27, Chrome 22, Internet Explorer 11, Opera 14, Safari 7, Android 4.4, and Java 8. "Intermediate 2018" is an intermediate set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. Select the Intermediate 2018 cipher suites if you require compatibility with a wider range of clients, legacy browsers, or older Linux tools.

Related Name

ssl.server.exclude.cipher.list

Default Value

modern2018

API Name

tls_ciphers

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Deploy Directory

Description

Whether to suppress configuration warnings produced by the Deploy Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_client_config_root_dir

Required

true

Suppress Configuration Validator: Allowed System Users

Description

Whether to suppress configuration warnings produced by the Allowed System Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_allowed_system_users

Required

true

Suppress Configuration Validator: Banned System Users

Description

Whether to suppress configuration warnings produced by the Banned System Users configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_banned_users

Required

true

Suppress Configuration Validator: Container Executor Group

Description

Whether to suppress configuration warnings produced by the Container Executor Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_container_executor_group

Required

true

Suppress Configuration Validator: NodeManager GPU Devices Allowed

Description

Whether to suppress configuration warnings produced by the NodeManager GPU Devices Allowed configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gpu_plugin_allowed_devices

Required

true

Suppress Configuration Validator: NodeManager GPU Detection Executable

Description

Whether to suppress configuration warnings produced by the NodeManager GPU Detection Executable configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_gpu_plugin_detector_path

Required

true

Suppress Configuration Validator: Running Job History Location

Description

Whether to suppress configuration warnings produced by the Running Job History Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_job_history_dir

Required

true

Suppress Configuration Validator: Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Hadoop Metrics2 Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hadoop_metrics2_safety_valve

Required

true

Suppress Configuration Validator: System Group

Description

Whether to suppress configuration warnings produced by the System Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_history_process_groupname

Required

true

Suppress Configuration Validator: System User

Description

Whether to suppress configuration warnings produced by the System User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_history_process_username

Required

true

Suppress Configuration Validator: I/O Sort Factor

Description

Whether to suppress configuration warnings produced by the I/O Sort Factor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_io_sort_factor

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: JobHistory Server Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the JobHistory Server Advanced Configuration Snippet (Safety Valve) for yarn-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_config_safety_valve

Required

true

Suppress Configuration Validator: JobHistory Server Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the JobHistory Server Advanced Configuration Snippet (Safety Valve) for mapred-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_mapred_safety_valve

Required

true

Suppress Configuration Validator: JobHistory Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the JobHistory Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jobhistory_role_env_safety_valve

Required

true

Suppress Configuration Validator: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the Role-Specific Kerberos Principal configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Configuration Validator: CGroups Hierarchy

Description

Whether to suppress configuration warnings produced by the CGroups Hierarchy configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_linux_container_executor_cgroups_hierarchy

Required

true

Suppress Configuration Validator: ResourceManager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the ResourceManager Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the Rules to Extract Events from Log Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Configuration Validator: Healthchecker Script Arguments

Description

Whether to suppress configuration warnings produced by the Healthchecker Script Arguments configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_healthchecker_script_args

Required

true

Suppress Configuration Validator: Healthchecker Script Path

Description

Whether to suppress configuration warnings produced by the Healthchecker Script Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_healthchecker_script_path

Required

true

Suppress Configuration Validator: Compression Codec of MapReduce Map Output

Description

Whether to suppress configuration warnings produced by the Compression Codec of MapReduce Map Output configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_map_output_compression_codec

Required

true

Suppress Configuration Validator: Compression Codec of MapReduce Job Output

Description

Whether to suppress configuration warnings produced by the Compression Codec of MapReduce Job Output configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapred_output_compression_codec

Required

true

Suppress Configuration Validator: MR Application Environment

Description

Whether to suppress configuration warnings produced by the MR Application Environment configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_admin_user_env

Required

true

Suppress Configuration Validator: Maximum Number of Attempts for MapReduce Jobs

Description

Whether to suppress configuration warnings produced by the Maximum Number of Attempts for MapReduce Jobs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_am_max_attempts

Required

true

Suppress Configuration Validator: MR Application Classpath

Description

Whether to suppress configuration warnings produced by the MR Application Classpath configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_application_classpath

Required

true

Suppress Configuration Validator: MR Application Framework Path

Description

Whether to suppress configuration warnings produced by the MR Application Framework Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_application_framework_path

Required

true

Suppress Configuration Validator: MapReduce Client Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the MapReduce Client Advanced Configuration Snippet (Safety Valve) for mapred-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_config_safety_valve

Required

true

Suppress Configuration Validator: Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh

Description

Whether to suppress configuration warnings produced by the Gateway Client Environment Advanced Configuration Snippet (Safety Valve) for hadoop-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_env_safety_valve

Required

true

Suppress Configuration Validator: Client Java Configuration Options

Description

Whether to suppress configuration warnings produced by the Client Java Configuration Options configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_client_java_opts

Required

true

Suppress Configuration Validator: ACL For Modifying A Job

Description

Whether to suppress configuration warnings produced by the ACL For Modifying A Job configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_acl_modify_job

Required

true

Suppress Configuration Validator: ACL For Viewing A Job

Description

Whether to suppress configuration warnings produced by the ACL For Viewing A Job configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_acl_view_job

Required

true

Suppress Configuration Validator: Redacted MapReduce Job Properties

Description

Whether to suppress configuration warnings produced by the Redacted MapReduce Job Properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_job_redacted_properties

Required

true

Suppress Configuration Validator: MapReduce JobHistory Server Port

Description

Whether to suppress configuration warnings produced by the MapReduce JobHistory Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_address

Required

true

Suppress Configuration Validator: MapReduce JobHistory Server Admin Interface Port

Description

Whether to suppress configuration warnings produced by the MapReduce JobHistory Server Admin Interface Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_admin_address

Required

true

Suppress Configuration Validator: MapReduce JobHistory Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the MapReduce JobHistory Web Application HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_webapp_address

Required

true

Suppress Configuration Validator: MapReduce JobHistory Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the MapReduce JobHistory Web Application HTTPS Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_jobhistory_webapp_https_address

Required

true

Suppress Configuration Validator: Map Task Java Opts Base

Description

Whether to suppress configuration warnings produced by the Map Task Java Opts Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_map_java_opts

Required

true

Suppress Configuration Validator: Map Task Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Map Task Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_map_java_opts_max_heap_mapreduce_map_memory_mb_validator

Required

true

Suppress Configuration Validator: Reduce Task Java Opts Base

Description

Whether to suppress configuration warnings produced by the Reduce Task Java Opts Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_reduce_java_opts

Required

true

Suppress Configuration Validator: Reduce Task Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Reduce Task Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_reduce_java_opts_max_heap_mapreduce_reduce_memory_mb_validator

Required

true

Suppress Configuration Validator: Job Submit Replication Validator

Description

Whether to suppress configuration warnings produced by the Job Submit Replication Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mapreduce_replication_validator

Required

true

Suppress Configuration Validator: Java Configuration Options for JobHistory Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for JobHistory Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mr2_jobhistory_java_opts

Required

true

Suppress Configuration Validator: JobHistory Server Log Directory

Description

Whether to suppress configuration warnings produced by the JobHistory Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mr2_jobhistory_log_dir

Required

true

Suppress Configuration Validator: Java Configuration Options for NodeManager

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for NodeManager configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_node_manager_java_opts

Required

true

Suppress Configuration Validator: NodeManager Log Directory

Description

Whether to suppress configuration warnings produced by the NodeManager Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_node_manager_log_dir

Required

true

Suppress Configuration Validator: NodeManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the NodeManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_config_safety_valve

Required

true

Suppress Configuration Validator: NodeManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the NodeManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_mapred_safety_valve

Required

true

Suppress Configuration Validator: NodeManager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the NodeManager Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_role_env_safety_valve

Required

true

Suppress Configuration Validator: NodeManager Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the NodeManager Web Application HTTPS Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_webserver_https_port

Required

true

Suppress Configuration Validator: NodeManager Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the NodeManager Web Application HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nodemanager_webserver_port

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Java Configuration Options for ResourceManager

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for ResourceManager configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resource_manager_java_opts

Required

true

Suppress Configuration Validator: ResourceManager Log Directory

Description

Whether to suppress configuration warnings produced by the ResourceManager Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resource_manager_log_dir

Required

true

Suppress Configuration Validator: Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_capacity_scheduler_configuration

Required

true

Suppress Configuration Validator: ResourceManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the ResourceManager Advanced Configuration Snippet (Safety Valve) for yarn-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_config_safety_valve

Required

true

Suppress Configuration Validator: Fair Scheduler XML Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Fair Scheduler XML Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_fair_scheduler_configuration

Required

true

Suppress Configuration Validator: ResourceManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the ResourceManager Advanced Configuration Snippet (Safety Valve) for mapred-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_mapred_safety_valve

Required

true

Suppress Configuration Validator: ResourceManager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the ResourceManager Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_role_env_safety_valve

Required

true

Suppress Configuration Validator: ResourceManager Web Application HTTPS Port (TLS/SSL)

Description

Whether to suppress configuration warnings produced by the ResourceManager Web Application HTTPS Port (TLS/SSL) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_webserver_https_port

Required

true

Suppress Configuration Validator: ResourceManager Web Application HTTP Port

Description

Whether to suppress configuration warnings produced by the ResourceManager Web Application HTTP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_resourcemanager_webserver_port

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_allow.txt

Description

Whether to suppress configuration warnings produced by the ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_allow.txt configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_hosts_allow_safety_valve

Required

true

Suppress Configuration Validator: ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_exclude.txt

Description

Whether to suppress configuration warnings produced by the ResourceManager Advanced Configuration Snippet (Safety Valve) for nodes_exclude.txt configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_hosts_exclude_safety_valve

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: ApplicationMaster Environment

Description

Whether to suppress configuration warnings produced by the ApplicationMaster Environment configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_admin_user_env

Required

true

Suppress Configuration Validator: ApplicationMaster Java Opts Base

Description

Whether to suppress configuration warnings produced by the ApplicationMaster Java Opts Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_command_opts

Required

true

Suppress Configuration Validator: ApplicationMaster Java Maximum Heap Size Validator

Description

Whether to suppress configuration warnings produced by the ApplicationMaster Java Maximum Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_max_heap_yarn_app_mapreduce_am_resource_mb_validator

Required

true

Suppress Configuration Validator: MapReduce ApplicationMaster Staging Root Directory

Description

Whether to suppress configuration warnings produced by the MapReduce ApplicationMaster Staging Root Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_app_mapreduce_am_staging_dir

Required

true

Suppress Configuration Validator: YARN Client Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the YARN Client Advanced Configuration Snippet (Safety Valve) for yarn-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_client_config_safety_valve

Required

true

Suppress Configuration Validator: Allowed Devices for Docker Containers

Description

Whether to suppress configuration warnings produced by the Allowed Devices for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_devices

Required

true

Suppress Configuration Validator: Allowed Read-Only Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the Allowed Read-Only Mounts for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_ro_mounts

Required

true

Suppress Configuration Validator: Allowed Read-Write Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the Allowed Read-Write Mounts for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_rw_mounts

Required

true

Suppress Configuration Validator: Allowed Volume Drivers for Docker Containers

Description

Whether to suppress configuration warnings produced by the Allowed Volume Drivers for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_allowed_volume_drivers

Required

true

Suppress Configuration Validator: Docker Binary Path

Description

Whether to suppress configuration warnings produced by the Docker Binary Path configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_binary

Required

true

Suppress Configuration Validator: Validates configuration of YARN NodeManagers when Docker on YARN feature is enabled.

Description

Whether to suppress configuration warnings produced by the Validates configuration of YARN NodeManagers when Docker on YARN feature is enabled. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_on_yarn_validator

Required

true

Suppress Configuration Validator: Trusted Registries for Docker Containers

Description

Whether to suppress configuration warnings produced by the Trusted Registries for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_docker_trusted_registries

Required

true

Suppress Configuration Validator: YARN FPGA Resources Validator

Description

Whether to suppress configuration warnings produced by the YARN FPGA Resources Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_fpga_validator

Required

true

Suppress Configuration Validator: YARN GPU Resources Validator

Description

Whether to suppress configuration warnings produced by the YARN GPU Resources Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_gpu_validator

Required

true

Suppress Configuration Validator: NodeManager IPC Address

Description

Whether to suppress configuration warnings produced by the NodeManager IPC Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_address

Required

true

Suppress Configuration Validator: Containers Environment Variable

Description

Whether to suppress configuration warnings produced by the Containers Environment Variable configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_admin_env

Required

true

Suppress Configuration Validator: Containers Environment Variables Whitelist

Description

Whether to suppress configuration warnings produced by the Containers Environment Variables Whitelist configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_env_whitelist

Required

true

Suppress Configuration Validator: FPGA initializer script

Description

Whether to suppress configuration warnings produced by the FPGA initializer script configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_fpga_plugin_initializer_script

Required

true

Suppress Configuration Validator: NodeManager Local Directories

Description

Whether to suppress configuration warnings produced by the NodeManager Local Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_local_dirs

Required

true

Suppress Configuration Validator: Localizer Port

Description

Whether to suppress configuration warnings produced by the Localizer Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_localizer_address

Required

true

Suppress Configuration Validator: Minimum Hard Limit for Log Aggregation Roll Monitoring Interval

Description

Whether to suppress configuration warnings produced by the Minimum Hard Limit for Log Aggregation Roll Monitoring Interval configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds_min

Required

true

Suppress Configuration Validator: Log Aggregation Roll Monitoring Interval Minimum Validator

Description

Whether to suppress configuration warnings produced by the Log Aggregation Roll Monitoring Interval Minimum Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_aggregation_roll_monitoring_interval_seconds_minimum_validator

Required

true

Suppress Configuration Validator: NodeManager Container Log Directories

Description

Whether to suppress configuration warnings produced by the NodeManager Container Log Directories configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_log_dirs

Required

true

Suppress Configuration Validator: NodeManager Recovery Directory

Description

Whether to suppress configuration warnings produced by the NodeManager Recovery Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_recovery_dir

Required

true

Suppress Configuration Validator: Remote App Log Directory

Description

Whether to suppress configuration warnings produced by the Remote App Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_remote_app_log_dir

Required

true

Suppress Configuration Validator: Remote App Log Directory Suffix

Description

Whether to suppress configuration warnings produced by the Remote App Log Directory Suffix configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_remote_app_log_dir_suffix

Required

true

Suppress Configuration Validator: Allowed FPGA devices

Description

Whether to suppress configuration warnings produced by the Allowed FPGA devices configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_allowed_fpga_devices

Required

true

Suppress Configuration Validator: List of available FPGA devices

Description

Whether to suppress configuration warnings produced by the List of available FPGA devices configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_available_devices

Required

true

Suppress Configuration Validator: Path to FPGA (aocl) tool

Description

Whether to suppress configuration warnings produced by the Path to FPGA (aocl) tool configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_resource_plugins_fpga_path_to_discovery_executables

Required

true

Suppress Configuration Validator: Allowed Linux Runtimes

Description

Whether to suppress configuration warnings produced by the Allowed Linux Runtimes configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_allowed_runtimes

Required

true

Suppress Configuration Validator: Allowed Docker Container Networks

Description

Whether to suppress configuration warnings produced by the Allowed Docker Container Networks configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_allowed_container_networks

Required

true

Suppress Configuration Validator: Docker Capabilities

Description

Whether to suppress configuration warnings produced by the Docker Capabilities configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_capabilities

Required

true

Suppress Configuration Validator: Default Docker Container Network

Description

Whether to suppress configuration warnings produced by the Default Docker Container Network configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_container_network

Required

true

Suppress Configuration Validator: Default Read-Only Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the Default Read-Only Mounts for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_ro_mounts

Required

true

Suppress Configuration Validator: Default Read-Write Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the Default Read-Write Mounts for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_rw_mounts

Required

true

Suppress Configuration Validator: Default Tempfs Mounts for Docker Containers

Description

Whether to suppress configuration warnings produced by the Default Tempfs Mounts for Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_default_tmpfs_mounts

Required

true

Suppress Configuration Validator: ACL for Privileged Docker Containers

Description

Whether to suppress configuration warnings produced by the ACL for Privileged Docker Containers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_nodemanager_runtime_linux_docker_privileged_containers_acl

Required

true

Suppress Configuration Validator: ResourceManager Address

Description

Whether to suppress configuration warnings produced by the ResourceManager Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_address

Required

true

Suppress Configuration Validator: Administration Address

Description

Whether to suppress configuration warnings produced by the Administration Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_admin_address

Required

true

Suppress Configuration Validator: ApplicationMaster Maximum Attempts

Description

Whether to suppress configuration warnings produced by the ApplicationMaster Maximum Attempts configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_am_max_retries

Required

true

Suppress Configuration Validator: Resource Tracker Address

Description

Whether to suppress configuration warnings produced by the Resource Tracker Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_resource_tracker_address

Required

true

Suppress Configuration Validator: Scheduler Address

Description

Whether to suppress configuration warnings produced by the Scheduler Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resourcemanager_scheduler_address

Required

true

Suppress Configuration Validator: YARN Resource Types Validator

Description

Whether to suppress configuration warnings produced by the YARN Resource Types Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_resources_validator

Required

true

Suppress Parameter Validation: Cloudera Manager Container Usage Metrics Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Container Usage Metrics Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cm_yarn_container_usage_input_dir

Required

true

Suppress Parameter Validation: Container Usage MapReduce Job Pool

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Usage MapReduce Job Pool parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cm_yarn_container_usage_job_pool

Required

true

Suppress Parameter Validation: Container Usage MapReduce Job User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Usage MapReduce Job User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cm_yarn_container_usage_job_user

Required

true

Suppress Parameter Validation: Container Usage Output Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Container Usage Output Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_cm_yarn_container_usage_output_dir

Required

true

Suppress Configuration Validator: Gateway Count Validator

Description

Whether to suppress configuration warnings produced by the Gateway Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_gateway_count_validator

Required

true

Suppress Configuration Validator: Secure Web UI Validator

Description

Whether to suppress configuration warnings produced by the Secure Web UI Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_secure_web_ui

Required

true

Suppress Configuration Validator: Hadoop TLS/SSL Validator

Description

Whether to suppress configuration warnings produced by the Hadoop TLS/SSL Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hadoop_ssl_validator

Required

true

Suppress Parameter Validation: System User's Home Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User's Home Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_hdfs_user_home_dir

Required

true

Suppress Configuration Validator: JobHistory Server Count Validator

Description

Whether to suppress configuration warnings produced by the JobHistory Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_jobhistory_count_validator

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: Llama Proxy User Groups

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Llama Proxy User Groups parameter.

Related Name

Default Value

false

API Name

service_config_suppression_llama_proxy_user_groups_list

Required

true

Suppress Parameter Validation: Llama Proxy User Hosts

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Llama Proxy User Hosts parameter.

Related Name

Default Value

false

API Name

service_config_suppression_llama_proxy_user_hosts_list

Required

true

Suppress Parameter Validation: Hive LLAP Kerberos Conf Staging Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hive LLAP Kerberos Conf Staging Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_llap_kerberos_staging_path

Required

true

Suppress Parameter Validation: HDFS Replication Advanced Configuration Snippet (Safety Valve) for mapred-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Advanced Configuration Snippet (Safety Valve) for mapred-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_mapreduce_service_replication_config_safety_valve

Required

true

Suppress Configuration Validator: NodeManager Count Validator

Description

Whether to suppress configuration warnings produced by the NodeManager Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_nodemanager_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Ranger DFS Audit Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger DFS Audit Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_dir

Required

true

Suppress Parameter Validation: Ranger Audit DFS Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit DFS Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_hdfs_spool_dir

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-audit.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-audit.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_safety_valve

Required

true

Suppress Parameter Validation: Ranger Audit Solr Spool Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Audit Solr Spool Dir parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_audit_solr_spool_dir

Required

true

Suppress Parameter Validation: Ranger Plugin Trusted Proxy IP Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Plugin Trusted Proxy IP Address parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_plugin_trusted_proxy_ipaddress

Required

true

Suppress Parameter Validation: Ranger Policy Cache Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Ranger Policy Cache Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policy_cache_dir

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-policymgr-ssl.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-policymgr-ssl.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_policymgr_ssl_safety_valve

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-security.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for ranger-yarn-security.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ranger_security_safety_valve

Required

true

Suppress Configuration Validator: ResourceManager Count Validator

Description

Whether to suppress configuration warnings produced by the ResourceManager Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_resourcemanager_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Client Config Overrides

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Client Config Overrides parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_client_config_overrides

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: TLS/SSL Client Truststore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Client Truststore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: TLS/SSL Client Truststore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Client Truststore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Hadoop TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Hadoop TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Admin ACL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin ACL parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_admin_acl

Required

true

Suppress Parameter Validation: YARN Application Aggregates

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Application Aggregates parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_application_aggregates

Required

true

Suppress Parameter Validation: YARN Application Classpath

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Application Classpath parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_application_classpath

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for core-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for core-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_core_site_safety_valve

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for hadoop-policy.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_hadoop_policy_config_safety_valve

Required

true

Suppress Parameter Validation: Supported Log Aggregation File Formats

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Supported Log Aggregation File Formats parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_log_aggregation_file_formats

Required

true

Suppress Parameter Validation: Remote App Log Directory for IFile Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory for IFile Format parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_log_aggregation_ifile_remote_app_log_dir

Required

true

Suppress Parameter Validation: Remote App Log Directory Suffix for IFile Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory Suffix for IFile Format parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_log_aggregation_ifile_remote_app_log_dir_suffix

Required

true

Suppress Parameter Validation: Remote App Log Directory for TFile Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory for TFile Format parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_log_aggregation_tfile_remote_app_log_dir

Required

true

Suppress Parameter Validation: Remote App Log Directory Suffix for TFile Format

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote App Log Directory Suffix for TFile Format parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_log_aggregation_tfile_remote_app_log_dir_suffix

Required

true

Suppress Parameter Validation: UNIX User for Nonsecure Mode with Linux Container Executor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the UNIX User for Nonsecure Mode with Linux Container Executor parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_nodemanager_linux_container_executor_nonsecure_mode_local_user

Required

true

Suppress Configuration Validator: Yarn Queue Manager Validator

Description

Whether to suppress configuration warnings produced by the Yarn Queue Manager Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_queue_manager_validator

Required

true

Suppress Configuration Validator: YARN Resource Types Validator

Description

Whether to suppress configuration warnings produced by the YARN Resource Types Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_resources_validator

Required

true

Suppress Parameter Validation: RM-HA Cluster ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the RM-HA Cluster ID parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_rm_ha_cluster_id

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_service_config_safety_valve

Required

true

Suppress Parameter Validation: YARN Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_service_env_safety_valve

Required

true

Suppress Parameter Validation: YARN Service MapReduce Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service MapReduce Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_service_mapred_safety_valve

Required

true

Suppress Parameter Validation: HDFS Replication Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Replication Advanced Configuration Snippet (Safety Valve) for yarn-site.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_service_replication_config_safety_valve

Required

true

Suppress Parameter Validation: YARN Services Dependencies Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Services Dependencies Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_services_framework_path

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_ssl_client_safety_valve

Required

true

Suppress Parameter Validation: YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Service Advanced Configuration Snippet (Safety Valve) for ssl-server.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_yarn_ssl_server_safety_valve

Required

true

Suppress Health Test: JobHistory Server Health

Description

Whether to suppress the results of the JobHistory Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_yarn_jobhistory_health

Required

true

Suppress Health Test: NodeManager Health

Description

Whether to suppress the results of the NodeManager Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_yarn_node_managers_healthy

Required

true

Suppress Health Test: ResourceManager Health

Description

Whether to suppress the results of the ResourceManager Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_yarn_resourcemanagers_health

Required

true

Suppress Health Test: YARN Container Usage Aggregation

Description

Whether to suppress the results of the YARN Container Usage Aggregation heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_yarn_usage_aggregation_health

Required

true

YARN Services Management

Enable YARN Services

Description

Configure YARN to support yarn managed services, enabling this will allow users to create long running YARN services like LLAP.

Related Name

Default Value

true

API Name

yarn_services_enabled

Required

false

YARN Services Dependencies Path

Description

This is the path where the YARN services dependencies tarball should be uploaded.

Related Name

yarn.service.framework.path

Default Value

/user/yarn/services/service-framework/$cdhVersion/service-dep.tar.gz

API Name

yarn_services_framework_path

Required

false

YARN Queue Manager Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

YARN Queue Manager Service Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

For advanced use only, a string to be inserted into conf/webapp.properties. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

conf/webapp.properties_service_safety_valve

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

hadoop

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

yarn

API Name

process_username

Required

true

YARN Queue Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

QUEUEMANAGER_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Enable Kerberos Authentication

Description

Specifies that the Hadoop cluster is secured using Kerberos authentication.

Related Name

kerberos.auth.enabled

Default Value

false

API Name

kerberos.auth.enabled

Required

false

System User's Home Directory

Description

The home directory of the system user on the local filesystem. Since Queue Manager uses Yarn user, make sure this value is same as yarn user directory.

Related Name

queuemanager_user_home_dir

Default Value

/var/lib/hadoop-yarn

API Name

queuemanager_user_home_dir

Required

false

ZooKeeper Service

Description

Name of the ZooKeeper service that this YARN Queue Manager service instance depends on

Related Name

Default Value

API Name

zookeeper_service

Required

true

Ports and Addresses

Config Service Application Connector Port

Description

Application connector port for config service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_application_connector_port

Default Value

8080

API Name

config_service_application_connector_port

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

yarn

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/external_cpx.properties

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/external_cpx.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/external_cpx.properties_role_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/quartz.properties

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/quartz.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/quartz.properties_role_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_conf/webapp.properties_role_safety_valve

Required

true

Suppress Configuration Validator: Config Service Admin Connector Port

Description

Whether to suppress configuration warnings produced by the Config Service Admin Connector Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_config_service_admin_connector_port

Required

true

Suppress Configuration Validator: Location for config-service DB

Description

Whether to suppress configuration warnings produced by the Location for config-service DB configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_config_service_db_loc

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Log Directory

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for property_configs

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for property_configs configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_property_configs_role_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Store Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Store Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_store_role_env_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Port

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_webapp_port

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_webapp_role_env_safety_valve

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for scheduling_rules

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for scheduling_rules configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_scheduling_rules_role_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: YARN Queue Manager Service Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Service Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties parameter.

Related Name

Default Value

false

API Name

service_config_suppression_conf/webapp.properties_service_safety_valve

Required

true

Suppress Parameter Validation: Config Service Application Connector Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Config Service Application Connector Port parameter.

Related Name

Default Value

false

API Name

service_config_suppression_config_service_application_connector_port

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: YARN Queue Manager Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_queuemanager_service_env_safety_valve

Required

true

Suppress Configuration Validator: YARN Queue Manager Store Count Validator

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Store Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_queuemanager_store_count_validator

Required

true

Suppress Parameter Validation: System User's Home Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User's Home Directory parameter.

Related Name

Default Value

false

API Name

service_config_suppression_queuemanager_user_home_dir

Required

true

Suppress Configuration Validator: YARN Queue Manager Webapp Count Validator

Description

Whether to suppress configuration warnings produced by the YARN Queue Manager Webapp Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_queuemanager_webapp_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

YARN Queue Manager Store

Advanced

YARN Queue Manager Store Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

For advanced use only. A string to be inserted into conf/webapp.properties for this role only.

Related Name

Default Value

API Name

conf/webapp.properties_role_safety_valve

Required

false

YARN Queue Manager Store Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

YARN Queue Manager Store Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

QUEUEMANAGER_STORE_role_env_safety_valve

Required

false

Logs

YARN Queue Manager Store Log Directory

Description

The log directory for log files of the role YARN Queue Manager Store.

Related Name

yarn_queuemanager_store_log_dir

Default Value

/var/log/yarn/queuemanager

API Name

log_dir

Required

false

YARN Queue Manager Store Logging Threshold

Description

The minimum log level for YARN Queue Manager Store logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

YARN Queue Manager Store Maximum Log File Backups

Description

The maximum number of rolled log files to keep for YARN Queue Manager Store logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

YARN Queue Manager Store Max Log Size

Description

The maximum size, in megabytes, per log file for YARN Queue Manager Store logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

queuemanager_store_fd_thresholds

Required

false

YARN Queue Manager Store Host Health Test

Description

When computing the overall YARN Queue Manager Store health, consider the host's health.

Related Name

Default Value

true

API Name

queuemanager_store_host_health_enabled

Required

false

YARN Queue Manager Store Process Health Test

Description

Enables the health test that the YARN Queue Manager Store's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

queuemanager_store_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Config Service Admin Max Threads.

Description

The maximum number of threads to use for admin requests in config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_admin_max_threads

Default Value

64

API Name

config_service_admin_max_threads

Required

false

Config Service Admin Min Threads.

Description

The minimum number of threads to use for admin requests in config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_admin_min_threads

Default Value

1

API Name

config_service_admin_min_threads

Required

false

Location for config-service DB

Description

If you change the config-service DB location value then you need to perform a manual migration step, as explained in the database migration documentation of config-service.

Related Name

config_service_db_loc

Default Value

API Name

config_service_db_loc

Required

false

Config Service Header Cache Size

Description

Header cache size in bytes for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_header_cache_size

Default Value

512

API Name

config_service_header_cache_size

Required

false

Config Service Idle Timeout

Description

The maximum idle time for a connection in config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_idle_timeout

Default Value

30

API Name

config_service_idle_timeout

Required

false

Config Service Input Buffer Size

Description

Input buffer size in kibibytes for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_input_buffer_size

Default Value

8

API Name

config_service_input_buffer_size

Required

false

Config Service Maximum Buffer Size

Description

Maximum buffer size in kibibytes for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_max_buffer_size

Default Value

64

API Name

config_service_max_buffer_size

Required

false

Config Service Max Request Header Size

Description

Maximum HTTP request header size for the config-service in KiB. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_max_request_header_size

Default Value

8

API Name

config_service_max_request_header_size

Required

false

Config Service Max Response Header Size

Description

Maximum HTTP response header size for the config-service in KiB. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_max_response_header_size

Default Value

8

API Name

config_service_max_response_header_size

Required

false

Config Service Min Bufferpool Size

Description

Min bufferpool size in bytes for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_min_buffer_pool_size

Default Value

8

API Name

config_service_min_buffer_pool_size

Required

false

Config Service Output Buffer Size

Description

Output buffer size in kibibytes for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_output_buffer_size

Default Value

32

API Name

config_service_output_buffer_size

Required

false

YARN Queue Manager Store Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Config Service Admin Connector Port

Description

Admin connector port for config-service. For more information about this jetty property, please refer to the configuration documentation of dropwizard.

Related Name

config_service_admin_connector_port

Default Value

8081

API Name

config_service_admin_connector_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable TLS/SSL for YARN Queue Manager Store

Description

Encrypt communication between clients and YARN Queue Manager Store using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

queuemanager_store_ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

YARN Queue Manager Store TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when YARN Queue Manager Store is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

queuemanager_store_keystore_file

Default Value

API Name

ssl_server_keystore_location

Required

false

YARN Queue Manager Store TLS/SSL Server Keystore File Password

Description

The password for the YARN Queue Manager Store keystore file.

Related Name

queuemanager_store_password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: YARN Queue Manager Store Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/webapp.properties_role_safety_valve

Required

true

Suppress Parameter Validation: Config Service Admin Connector Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Config Service Admin Connector Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_config_service_admin_connector_port

Required

true

Suppress Parameter Validation: Location for config-service DB

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Location for config-service DB parameter.

Related Name

Default Value

false

API Name

role_config_suppression_config_service_db_loc

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: YARN Queue Manager Store Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Store Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: YARN Queue Manager Store Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_store_role_env_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: YARN Queue Manager Store TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: YARN Queue Manager Store TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Store TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_store_unexpected_exits

Required

true

YARN Queue Manager Webapp

Advanced

YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/external_cpx.properties

Description

For advanced use only. A string to be inserted into conf/external_cpx.properties for this role only.

Related Name

Default Value

API Name

conf/external_cpx.properties_role_safety_valve

Required

false

YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/quartz.properties

Description

For advanced use only. A string to be inserted into conf/quartz.properties for this role only.

Related Name

Default Value

API Name

conf/quartz.properties_role_safety_valve

Required

false

YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

For advanced use only. A string to be inserted into conf/webapp.properties for this role only.

Related Name

Default Value

API Name

conf/webapp.properties_role_safety_valve

Required

false

YARN Queue Manager Webapp Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for property_configs

Description

For advanced use only. A string to be inserted into property_configs for this role only.

Related Name

Default Value

API Name

property_configs_role_safety_valve

Required

false

YARN Queue Manager Webapp Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

QUEUEMANAGER_WEBAPP_role_env_safety_valve

Required

false

YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for scheduling_rules

Description

For advanced use only. A string to be inserted into scheduling_rules for this role only.

Related Name

Default Value

API Name

scheduling_rules_role_safety_valve

Required

false

Logs

YARN Queue Manager Webapp Log Directory

Description

The log directory for log files of the role YARN Queue Manager Webapp.

Related Name

yarn_queuemanager_webapp_log_dir

Default Value

/var/log/yarn/queuemanager

API Name

log_dir

Required

false

YARN Queue Manager Webapp Logging Threshold

Description

The minimum log level for YARN Queue Manager Webapp logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

YARN Queue Manager Webapp Maximum Log File Backups

Description

The maximum number of rolled log files to keep for YARN Queue Manager Webapp logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

YARN Queue Manager Webapp Max Log Size

Description

The maximum size, in megabytes, per log file for YARN Queue Manager Webapp logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.

- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

queuemanager_webapp_fd_thresholds

Required

false

YARN Queue Manager Webapp Host Health Test

Description

When computing the overall YARN Queue Manager Webapp health, consider the host's health.

Related Name

Default Value

true

API Name

queuemanager_webapp_host_health_enabled

Required

false

YARN Queue Manager Webapp Process Health Test

Description

Enables the health test that the YARN Queue Manager Webapp's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

queuemanager_webapp_scm_health_enabled

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.

- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

YARN Queue Manager Webapp Diagnostics Collection Timeout

Description

The timeout in milliseconds to wait for diagnostics collection to complete.

Related Name

Default Value

5 minute(s)

API Name

csd_role_diagnostics_timeout

Required

false

YARN Queue Manager Accept Queue Size

Description

Accept queue size for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_accept_queue_size

Default Value

API Name

queuemanager_accept_queue_size

Required

false

YARN Queue Manager Accepted Receive Buffer Size

Description

Accepted receive buffer size for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_accepted_receive_buffer_size

Default Value

API Name

queuemanager_accepted_receive_buffer_size

Required

false

YARN Queue Manager Accepted Send Buffer Size

Description

Accepted Send Buffer Size for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_accepted_send_buffer_size

Default Value

API Name

queuemanager_accepted_send_buffer_size

Required

false

YARN Queue Manager Header Cache Size

Description

Header size for the Queue Manager Webapp in Bytes. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_header_cache_size

Default Value

API Name

queuemanager_header_cache_size

Required

false

YARN Queue Manager Idle Timeout

Description

Idle timeout for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_idle_timeout

Default Value

API Name

queuemanager_idle_timeout

Required

false

YARN Queue Manager Minimum Request Datarate

Description

Minimum request datarate for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_min_request_datarate

Default Value

API Name

queuemanager_min_request_datarate

Required

false

YARN Queue Manager Minimum Response Datarate

Description

Min response datarate for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_min_response_datarate

Default Value

API Name

queuemanager_min_response_datarate

Required

false

YARN Queue Manager Output Buffer Size

Description

Output buffer size for the Queue Manager Webapp in Bytes. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_output_buffer_size

Default Value

API Name

queuemanager_output_buffer_size

Required

false

YARN Queue Manager Request Header Size

Description

Maximum HTTP request header size for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_request_header_size

Default Value

API Name

queuemanager_request_header_size

Required

false

YARN Queue Manager Response Header Size

Description

Maximum HTTP response header size for the Queue Manager Webapp in Bytes. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_response_header_size

Default Value

API Name

queuemanager_response_header_size

Required

false

YARN Queue Manager Send Server Version

Description

Send server version for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_send_server_version

Default Value

true

API Name

queuemanager_send_server_version

Required

false

YARN Queue Manager Stop Timeout

Description

Stop timeout for the Queue Manager Webapp. For more information about this Jetty property, please refer to the Jetty documentation.

Related Name

queuemanager_stop_timeout

Default Value

API Name

queuemanager_stop_timeout

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

YARN Queue Manager Webapp Port

Description

The port that the YARN Queue Manager Webapp user interface listens on.

Related Name

queuemanager_webapp_port

Default Value

8082

API Name

queuemanager_webapp_port

Required

true

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

YARN Queue Manager Webapp TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that YARN Queue Manager Webapp might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

queuemanager.webapp.ssl.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

YARN Queue Manager Webapp TLS/SSL Trust Store Password

Description

The password for the YARN Queue Manager Webapp TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

queuemanager.webapp.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for YARN Queue Manager Webapp

Description

Encrypt communication between clients and YARN Queue Manager Webapp using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

queuemanager_webapp_ssl_enabled

Default Value

false

API Name

ssl_enabled

Required

false

YARN Queue Manager Webapp TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when YARN Queue Manager Webapp is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

queuemanager_webapp_keystore_file

Default Value

API Name

ssl_server_keystore_location

Required

false

YARN Queue Manager Webapp TLS/SSL Server Keystore File Password

Description

The password for the YARN Queue Manager Webapp keystore file.

Related Name

queuemanager_keystore_password

Default Value

API Name

ssl_server_keystore_password

Required

false

Supported SSL/TLS versions

Description

The SSL/TLS protocol versions to accept HTTPS connections from. Note that the available cipher suites also affect which protocol versions can be negotiated, and some cipher suites are only available in higher versions.

Related Name

queuemanager_includedProtocols

Default Value

TLSv1.2

API Name

supported_tls_versions

Required

false

SSL/TLS Cipher Suite

Description

The SSL/TLS cipher suites to use. "Modern 2018" is a modern set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. These cipher suites use strong cryptography and are preferred unless interaction with older clients is required. These modern cipher suites are compatible with Firefox 27, Chrome 22, Internet Explorer 11, Opera 14, Safari 7, Android 4.4, and Java 8. "Intermediate 2018" is an intermediate set of cipher suites as of 2018, according to the Mozilla server-side TLS recommendations. Select the Intermediate 2018 cipher suites if you require compatibility with a wider range of clients, legacy browsers, or older Linux tools.

Related Name

queuemanager_includedCipherSuites

Default Value

modern2018

API Name

tls_ciphers

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/external_cpx.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/external_cpx.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/external_cpx.properties_role_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/quartz.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/quartz.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/quartz.properties_role_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for conf/webapp.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_conf/webapp.properties_role_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for property_configs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for property_configs parameter.

Related Name

Default Value

false

API Name

role_config_suppression_property_configs_role_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_webapp_port

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_queuemanager_webapp_role_env_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for scheduling_rules

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp Advanced Configuration Snippet (Safety Valve) for scheduling_rules parameter.

Related Name

Default Value

false

API Name

role_config_suppression_scheduling_rules_role_safety_valve

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: YARN Queue Manager Webapp TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN Queue Manager Webapp TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_queuemanager_queuemanager_webapp_unexpected_exits

Required

true

Zeppelin Properties in Cloudera Runtime 7.2.18

Role groups:

Service-Wide

Advanced

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

zeppelin

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

zeppelin

API Name

process_username

Required

true

Zeppelin Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

ZEPPELIN_service_env_safety_valve

Required

false

Monitoring

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Zeppelin Server Role Health Test

Description

When computing the overall ZEPPELIN health, consider Zeppelin Server's health

Related Name

Default Value

true

API Name

ZEPPELIN_ZEPPELIN_SERVER_health_enabled

Required

false

Other

HDFS Service

Description

Name of the HDFS service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

hdfs_service

Required

true

Knox Service

Description

Name of the Knox service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

knox_service

Required

false

Livy for Spark 3 Service

Description

Name of the Livy for Spark 3 service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

livy_for_spark3_service

Required

false

Livy Service

Description

Name of the Livy service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

livy_service

Required

false

Spark Service

Description

Name of the Spark service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

spark_on_yarn_service

Required

true

YARN Service

Description

Name of the YARN service that this Zeppelin service instance depends on

Related Name

Default Value

API Name

yarn_service

Required

true

Zeppelin Authentication Method

Description

Indicates whether Kerberos is enabled.

Related Name

zeppelin.authentication.method.kerberos

Default Value

false

API Name

zeppelin.authentication.method.kerberos

Required

false

Security

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

zeppelin

API Name

kerberos_princ_name

Required

true

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Zeppelin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Zeppelin Server Log Directory

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Zeppelin Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Zeppelin Server TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Configuration Validator: Zeppelin Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Zeppelin Server TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Zeppelin Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Zeppelin Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Zeppelin Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Zeppelin Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-env.sh

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-env.sh configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin-conf/zeppelin-env.sh_role_safety_valve

Required

true

Suppress Configuration Validator: Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-site.xml

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-site.xml configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin-conf/zeppelin-site.xml_role_safety_valve

Required

true

Suppress Configuration Validator: Admin Group

Description

Whether to suppress configuration warnings produced by the Admin Group configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.admin.group

Required

true

Suppress Configuration Validator: Zeppelin Anonymous

Description

Whether to suppress configuration warnings produced by the Zeppelin Anonymous configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.anonymous.allowed

Required

true

Suppress Configuration Validator: Zeppelin Interpreter Config Location

Description

Whether to suppress configuration warnings produced by the Zeppelin Interpreter Config Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.config.fs.dir

Required

true

Suppress Configuration Validator: Zeppelin Config Storage Class

Description

Whether to suppress configuration warnings produced by the Zeppelin Config Storage Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.config.storage.class

Required

true

Suppress Configuration Validator: Zeppelin Local Repository Location

Description

Whether to suppress configuration warnings produced by the Zeppelin Local Repository Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.dep.localrepo

Required

true

Suppress Configuration Validator: Zeppelin Home Directory

Description

Whether to suppress configuration warnings produced by the Zeppelin Home Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.home.dir

Required

true

Suppress Configuration Validator: Zeppelin Interpreter Group Order

Description

Whether to suppress configuration warnings produced by the Zeppelin Interpreter Group Order configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.interpreter.group.order

Required

true

Suppress Configuration Validator: Zeppelin Local Repository Location

Description

Whether to suppress configuration warnings produced by the Zeppelin Local Repository Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.interpreter.localrepo

Required

true

Suppress Configuration Validator: Zeppelin Notebook Location

Description

Whether to suppress configuration warnings produced by the Zeppelin Notebook Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.notebook.dir

Required

true

Suppress Configuration Validator: Zeppelin Notebook Storage Class

Description

Whether to suppress configuration warnings produced by the Zeppelin Notebook Storage Class configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.notebook.storage

Required

true

Suppress Configuration Validator: Zeppelin Server Bind Address

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Bind Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.server.addr

Required

true

Suppress Configuration Validator: Zeppelin Shiro Knox Main Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro Knox Main Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.knox.main.block

Required

true

Suppress Configuration Validator: Zeppelin Shiro Main Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro Main Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.main.block

Required

true

Suppress Configuration Validator: Zeppelin Shiro Main Session Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro Main Session Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.main.session.block

Required

true

Suppress Configuration Validator: Zeppelin Shiro Roles Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro Roles Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.roles.block

Required

true

Suppress Configuration Validator: Zeppelin Shiro Urls Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro Urls Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.urls.block

Required

true

Suppress Configuration Validator: Zeppelin Shiro User Block

Description

Whether to suppress configuration warnings produced by the Zeppelin Shiro User Block configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.user.block

Required

true

Suppress Configuration Validator: Zeppelin SSL Client Authentication

Description

Whether to suppress configuration warnings produced by the Zeppelin SSL Client Authentication configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.client.auth

Required

true

Suppress Configuration Validator: Zeppelin SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the Zeppelin SSL Keystore Type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.keystore.type

Required

true

Suppress Configuration Validator: Zeppelin SSL Truststore type

Description

Whether to suppress configuration warnings produced by the Zeppelin SSL Truststore type configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.truststore.type

Required

true

Suppress Configuration Validator: Zeppelin Temp Webapps Directory

Description

Whether to suppress configuration warnings produced by the Zeppelin Temp Webapps Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.war.tempdir

Required

true

Suppress Configuration Validator: Zeppelin Websocket Text Size

Description

Whether to suppress configuration warnings produced by the Zeppelin Websocket Text Size configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.websocket.max.text.message.size

Required

true

Suppress Configuration Validator: Zeppelin Server Port

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_port

Required

true

Suppress Configuration Validator: Zeppelin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Zeppelin Server SSL Port

Description

Whether to suppress configuration warnings produced by the Zeppelin Server SSL Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_ssl_port

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Configuration Validator: Zeppelin Server Count Validator

Description

Whether to suppress configuration warnings produced by the Zeppelin Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_zeppelin_server_count_validator

Required

true

Suppress Parameter Validation: Zeppelin Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zeppelin_service_env_safety_valve

Required

true

Suppress Health Test: Zeppelin Server Health

Description

Whether to suppress the results of the Zeppelin Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_zeppelin_zeppelin_zeppelin_server_health

Required

true

Zeppelin Server

Advanced

Zeppelin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

false

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-env.sh

Description

For advanced use only. A string to be inserted into zeppelin-conf/zeppelin-env.sh for this role only.

Related Name

Default Value

API Name

zeppelin-conf/zeppelin-env.sh_role_safety_valve

Required

false

Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-site.xml

Description

For advanced use only. A string to be inserted into zeppelin-conf/zeppelin-site.xml for this role only.

Related Name

Default Value

API Name

zeppelin-conf/zeppelin-site.xml_role_safety_valve

Required

false

Zeppelin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

ZEPPELIN_SERVER_role_env_safety_valve

Required

false

Logs

Zeppelin Server Log Directory

Description

The log directory for log files of the role Zeppelin Server.

Related Name

log_dir

Default Value

/var/log/zeppelin

API Name

log_dir

Required

false

Zeppelin Server Logging Threshold

Description

The minimum log level for Zeppelin Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Zeppelin Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Zeppelin Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Zeppelin Server Max Log Size

Description

The maximum size, in megabytes, per log file for Zeppelin Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

zeppelin_server_fd_thresholds

Required

false

Zeppelin Server Host Health Test

Description

When computing the overall Zeppelin Server health, consider the host's health.

Related Name

Default Value

true

API Name

zeppelin_server_host_health_enabled

Required

false

Zeppelin Server Process Health Test

Description

Enables the health test that the Zeppelin Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

zeppelin_server_scm_health_enabled

Required

false

Other

Admin Group

Description

Admin group for Zeppelin.

Related Name

zeppelin.admin.group

Default Value

admins

API Name

zeppelin.admin.group

Required

false

Zeppelin Anonymous

Description

Anonymous user allowed by default.

Related Name

zeppelin.anonymous.allowed

Default Value

false

API Name

zeppelin.anonymous.allowed

Required

false

Zeppelin Interpreter Config Location

Description

Location of config file.

Related Name

zeppelin.config.fs.dir

Default Value

file:///var/lib/zeppelin/conf

API Name

zeppelin.config.fs.dir

Required

false

Zeppelin Config Storage Class

Description

Config persistence layer implementation.

Related Name

zeppelin.config.storage.class

Default Value

org.apache.zeppelin.storage.FileSystemConfigStorage

API Name

zeppelin.config.storage.class

Required

false

Zeppelin Local Repository Location

Description

Local repository for dependency loader.

Related Name

zeppelin.dep.localrepo

Default Value

/var/lib/zeppelin/local-repo

API Name

zeppelin.dep.localrepo

Required

false

Zeppelin Home Directory

Description

Location of zeppelin home directory.

Related Name

zeppelin.home.dir

Default Value

/var/lib/zeppelin

API Name

zeppelin.home.dir

Required

false

Zeppelin Interpreter Group Order

Description

Zeppelin interpreter group order.

Related Name

zeppelin.interpreter.group.order

Default Value

livy, md, angular, sh, jdbc, spark

API Name

zeppelin.interpreter.group.order

Required

false

Zeppelin Local Repository Location

Description

Local repository for interpreter's additional dependency loading.

Related Name

zeppelin.interpreter.localRepo

Default Value

/var/lib/zeppelin/local-repo

API Name

zeppelin.interpreter.localRepo

Required

false

Zeppelin Notebook Location

Description

Path or URI for notebook persist.

Related Name

zeppelin.notebook.dir

Default Value

file:///var/lib/zeppelin/notebook

API Name

zeppelin.notebook.dir

Required

false

Zeppelin Notebook Public Access

Description

Make notebook public by default when created, private otherwise.

Related Name

zeppelin.notebook.public

Default Value

false

API Name

zeppelin.notebook.public

Required

false

Zeppelin Notebook Storage Class

Description

Versioned notebook persistence layer implementation.

Related Name

zeppelin.notebook.storage

Default Value

org.apache.zeppelin.notebook.repo.FileSystemNotebookRepo

API Name

zeppelin.notebook.storage

Required

false

Zeppelin Server Bind Address

Description

Zeppelin Server binding address.

Related Name

zeppelin.server.addr

Default Value

0.0.0.0

API Name

zeppelin.server.addr

Required

false

Zeppelin Shiro Knox Main Block

Description

Knox configuration for main block.

Related Name

zeppelin.shiro.knox.main.block

Default Value

krbRealm = org.apache.zeppelin.realm.kerberos.KerberosRealm krbRealm.principal=SPNEGO_PRINCIPAL krbRealm.keytab=KEYTAB_FILE krbRealm.nameRules=DEFAULT krbRealm.signatureSecretFile=CONF_DIR/http_secret krbRealm.tokenValidity=36000 krbRealm.cookieDomain=DOMAIN krbRealm.cookiePath=/ authc = org.apache.zeppelin.realm.kerberos.KerberosAuthenticationFilter

API Name

zeppelin.shiro.knox.main.block

Required

false

Zeppelin Shiro Main Block

Description

Content of main block.

Related Name

zeppelin.shiro.main.block

Default Value

pamRealm=org.apache.zeppelin.realm.PamRealm pamRealm.service=sshd

API Name

zeppelin.shiro.main.block

Required

false

Zeppelin Shiro Main Session Block

Description

Content of main session block.

Related Name

zeppelin.shiro.main.session.block

Default Value

sessionManager = org.apache.shiro.web.session.mgt.DefaultWebSessionManager cookie = org.apache.shiro.web.servlet.SimpleCookie cookie.name = JSESSIONID cookie.httpOnly = true sessionManager.sessionIdCookie = $cookie securityManager.sessionManager = $sessionManager securityManager.sessionManager.globalSessionTimeout = 86400000 shiro.loginUrl = /api/login

API Name

zeppelin.shiro.main.session.block

Required

false

Zeppelin Shiro Roles Block

Description

Content of roles block.

Related Name

zeppelin.shiro.roles.block

Default Value

API Name

zeppelin.shiro.roles.block

Required

false

Zeppelin Shiro Urls Block

Description

Content of urls block.

Related Name

zeppelin.shiro.urls.block

Default Value

/api/version = anon /api/interpreter/setting/restart/** = authc /api/interpreter/** = authc, roles[zeppelin_admin_group] /api/notebook-repositories/** = authc, roles[zeppelin_admin_group] /api/configurations/** = authc, roles[zeppelin_admin_group] /api/credential/** = authc, roles[zeppelin_admin_group] /api/admin/** = authc, roles[zeppelin_admin_group] /** = authc

API Name

zeppelin.shiro.urls.block

Required

false

Zeppelin Shiro User Block

Description

Content of user block.

Related Name

zeppelin.shiro.user.block

Default Value

API Name

zeppelin.shiro.user.block

Required

false

Zeppelin SSL Client Authentication

Description

Should client authentication be used for SSL connections?

Related Name

zeppelin.ssl.client.auth

Default Value

false

API Name

zeppelin.ssl.client.auth

Required

false

Zeppelin SSL Keystore Type

Description

The format of the given keystore (e.g. JKS or PKCS12).

Related Name

zeppelin.ssl.keystore.type

Default Value

jks

API Name

zeppelin.ssl.keystore.type

Required

false

Zeppelin SSL Truststore type

Description

The format of the given truststore (e.g. JKS or PKCS12). Defaults to the same type as the keystore type.

Related Name

zeppelin.ssl.truststore.type

Default Value

jks

API Name

zeppelin.ssl.truststore.type

Required

false

Zeppelin Temp Webapps Directory

Description

Location of jetty temporary directory.

Related Name

zeppelin.war.tempdir

Default Value

/var/lib/zeppelin/webapps

API Name

zeppelin.war.tempdir

Required

false

Zeppelin Websocket Text Size

Description

Size in characters of the maximum text message to be received by websocket. Defaults to 1024000.

Related Name

zeppelin.websocket.max.text.message.size

Default Value

1024000

API Name

zeppelin.websocket.max.text.message.size

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Zeppelin Server Port

Description

The port of the Zeppelin server.

Related Name

zeppelin.server.port

Default Value

8885

API Name

zeppelin_server_port

Required

false

Zeppelin Server SSL Port

Description

The SSL port of the Zeppelin server.

Related Name

zeppelin.server.ssl.port

Default Value

8886

API Name

zeppelin_server_ssl_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Zeppelin Server TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Zeppelin Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

zeppelin.ssl.truststore.path

Default Value

API Name

ssl_client_truststore_location

Required

false

Zeppelin Server TLS/SSL Trust Store Password

Description

The password for the Zeppelin Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

zeppelin.ssl.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Enable TLS/SSL for Zeppelin Server

Description

Encrypt communication between clients and Zeppelin Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

zeppelin.ssl

Default Value

false

API Name

ssl_enabled

Required

false

Zeppelin Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Zeppelin Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

zeppelin.ssl.keystore.path

Default Value

API Name

ssl_server_keystore_location

Required

false

Zeppelin Server TLS/SSL Server Keystore File Password

Description

The password for the Zeppelin Server keystore file.

Related Name

zeppelin.ssl.keystore.password

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Zeppelin Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Zeppelin Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Zeppelin Server TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Zeppelin Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_client_truststore_password

Required

true

Suppress Parameter Validation: Zeppelin Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Zeppelin Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-env.sh

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-env.sh parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin-conf/zeppelin-env.sh_role_safety_valve

Required

true

Suppress Parameter Validation: Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-site.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Advanced Configuration Snippet (Safety Valve) for zeppelin-conf/zeppelin-site.xml parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin-conf/zeppelin-site.xml_role_safety_valve

Required

true

Suppress Parameter Validation: Admin Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Group parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.admin.group

Required

true

Suppress Parameter Validation: Zeppelin Anonymous

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Anonymous parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.anonymous.allowed

Required

true

Suppress Parameter Validation: Zeppelin Interpreter Config Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Interpreter Config Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.config.fs.dir

Required

true

Suppress Parameter Validation: Zeppelin Config Storage Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Config Storage Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.config.storage.class

Required

true

Suppress Parameter Validation: Zeppelin Local Repository Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Local Repository Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.dep.localrepo

Required

true

Suppress Parameter Validation: Zeppelin Home Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Home Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.home.dir

Required

true

Suppress Parameter Validation: Zeppelin Interpreter Group Order

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Interpreter Group Order parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.interpreter.group.order

Required

true

Suppress Parameter Validation: Zeppelin Local Repository Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Local Repository Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.interpreter.localrepo

Required

true

Suppress Parameter Validation: Zeppelin Notebook Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Notebook Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.notebook.dir

Required

true

Suppress Parameter Validation: Zeppelin Notebook Storage Class

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Notebook Storage Class parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.notebook.storage

Required

true

Suppress Parameter Validation: Zeppelin Server Bind Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Bind Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.server.addr

Required

true

Suppress Parameter Validation: Zeppelin Shiro Knox Main Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro Knox Main Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.knox.main.block

Required

true

Suppress Parameter Validation: Zeppelin Shiro Main Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro Main Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.main.block

Required

true

Suppress Parameter Validation: Zeppelin Shiro Main Session Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro Main Session Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.main.session.block

Required

true

Suppress Parameter Validation: Zeppelin Shiro Roles Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro Roles Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.roles.block

Required

true

Suppress Parameter Validation: Zeppelin Shiro Urls Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro Urls Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.urls.block

Required

true

Suppress Parameter Validation: Zeppelin Shiro User Block

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Shiro User Block parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.shiro.user.block

Required

true

Suppress Parameter Validation: Zeppelin SSL Client Authentication

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin SSL Client Authentication parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.client.auth

Required

true

Suppress Parameter Validation: Zeppelin SSL Keystore Type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin SSL Keystore Type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.keystore.type

Required

true

Suppress Parameter Validation: Zeppelin SSL Truststore type

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin SSL Truststore type parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.ssl.truststore.type

Required

true

Suppress Parameter Validation: Zeppelin Temp Webapps Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Temp Webapps Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.war.tempdir

Required

true

Suppress Parameter Validation: Zeppelin Websocket Text Size

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Websocket Text Size parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin.websocket.max.text.message.size

Required

true

Suppress Parameter Validation: Zeppelin Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_port

Required

true

Suppress Parameter Validation: Zeppelin Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Zeppelin Server SSL Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Zeppelin Server SSL Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zeppelin_server_ssl_port

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_file_descriptor

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zeppelin_zeppelin_server_unexpected_exits

Required

true

ZooKeeper Properties in Cloudera Runtime 7.2.18

Role groups:

Server

Advanced

ZooKeeper 'Four Letter Word' Command Whitelist

Description

ZooKeeper responds to specific Four-Letter-Word diagnostic telnet commands on its client port. Here you can configure which commands should be accepted by the server. Use asterisk ('*') to enable all of them.

Related Name

4lw.commands.whitelist

Default Value

conf cons crst dirs dump envi gtmk ruok stmk srst srvr stat wchs mntr isro

API Name

4lw_commands_whitelist

Required

false

Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap When Out of Memory

Description

When set, generates a heap dump file when when an out-of-memory error occurs.

Related Name

Default Value

true

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SERVER_role_env_safety_valve

Required

false

Java Configuration Options for Zookeeper Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or

greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

zk_server_java_opts

Required

false

Server Advanced Configuration Snippet (Safety Valve) for zoo.cfg

Description

For advanced use only. A string to be inserted into zoo.cfg for this role only.

Related Name

Default Value

API Name

zookeeper_config_safety_valve

Required

false

Logs

Server Logging Threshold

Description

The minimum log level for Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Server Max Log Size

Description

The maximum size, in megabytes, per log file for Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

ZooKeeper Log Directory

Description

Directory where ZooKeeper will place its log files.

Related Name

Default Value

/var/log/zookeeper

API Name

zk_server_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

ZooKeeper Server Connection Count Thresholds

Description

The health check thresholds of the weighted average size of the ZooKeeper Server connection count over a recent period. See ZooKeeper Server Connection Count Monitoring Period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

zookeeper_server_connection_count_thresholds

Required

false

ZooKeeper Server Connection Count Monitoring Period

Description

The period to review when computing the moving average of the connection count. Specified in minutes.

Related Name

Default Value

3 minute(s)

API Name

zookeeper_server_connection_count_window

Required

false

Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Data Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

zookeeper_server_data_directory_free_space_absolute_thresholds

Required

false

Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Data Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

zookeeper_server_data_directory_free_space_percentage_thresholds

Required

false

Transaction Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Transaction Log Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

zookeeper_server_data_log_directory_free_space_absolute_thresholds

Required

false

Transaction Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Transaction Log Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Transaction Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

zookeeper_server_data_log_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

zookeeper_server_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

zookeeper_server_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

zookeeper_server_gc_duration_window

Required

false

Server Host Health Test

Description

When computing the overall Server health, consider the host's health.

Related Name

Default Value

true

API Name

zookeeper_server_host_health_enabled

Required

false

Maximum Latency Monitoring Thresholds

Description

The percentage thresholds of the ratio of the maximum request latency to the maximum client-negotiable session timeout since the server was started.

Related Name

Default Value

Warning: 75.0 %, Critical: 100.0 %

API Name

zookeeper_server_max_latency_thresholds

Required

false

ZooKeeper Server Outstanding Requests Thresholds

Description

The health check thresholds of the weighted average size of the ZooKeeper Server outstanding requests queue over a recent period. See ZooKeeper Server Outstanding Requests Monitoring Period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

zookeeper_server_outstanding_requests_thresholds

Required

false

ZooKeeper Server Outstanding Requests Monitoring Period

Description

The period to review when computing the moving average of the outstanding requests queue size. Specified in minutes.

Related Name

Default Value

3 minute(s)

API Name

zookeeper_server_outstanding_requests_window

Required

false

Quorum Membership Detection Window

Description

The tolerance window that will be used in the detection of a ZooKeeper server's membership in a quorum. Specified in minutes.

Related Name

Default Value

3 minute(s)

API Name

zookeeper_server_quorum_membership_detection_window

Required

false

Enable the Quorum Membership Check

Description

Enables the quorum membership check for this ZooKeeper Server.

Related Name

Default Value

true

API Name

zookeeper_server_quorum_membership_enabled

Required

false

Server Process Health Test

Description

Enables the health test that the Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

zookeeper_server_scm_health_enabled

Required

false

Other

Client Port Address

Description

The address (IPv4, IPv6, or hostname) to monitor for client connections. This is the address that clients attempt to connect to. This setting is optional, because by default, ZooKeeper binds in such a way that any connection to the client port for any address/interface/NIC on the server will be accepted.

Related Name

clientPortAddress

Default Value

API Name

clientPortAddress

Required

false

Data Directory

Description

The disk location that ZooKeeper will use to store its database snapshots.

Related Name

dataDir

Default Value

/var/lib/zookeeper

API Name

dataDir

Required

false

Transaction Log Directory

Description

The disk location that ZooKeeper will use to store its transaction logs.

Related Name

dataLogDir

Default Value

/var/lib/zookeeper

API Name

dataLogDir

Required

false

Enable JMX Agent

Description

Enables the JMX agent on the ZooKeeper server. Turning this off on any of the ZooKeeper servers that are part of a service will prevent Cloudera Manager from being able to monitor that server and may affect the monitoring provided on the entire service.

Related Name

Default Value

true

API Name

enable_jmx_agent

Required

false

Enable Authenticated Communication with the JMX Agent

Description

Enables authentication when interacting with the JMX agent on the ZooKeeper server.

Related Name

Default Value

false

API Name

enable_jmx_authentication

Required

false

Enable ZooKeeper Admin Server

Description

The AdminServer is an embedded HTTP server that provides a REST interface for different diagnostics commands in ZooKeeper. The results of the commands are returned in JSON. The AdminServer is optional to enable, you should consider it as an alternative to the 'Four-Letter-Word' telnet interface.

Related Name

admin.enableServer

Default Value

false

API Name

enable_zookeeper_admin_server

Required

false

Name of User with Read-Only access to the JMX Agent

Description

Specifies the name of the user that has read-only privileges when using password file based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

Default Value

monitorRole

API Name

jmx_passwd_file_readonly_user

Required

false

Password of User with Read-Only Access to the JMX agent

Description

Specifies the password of the user that has read-only privileges when using password file based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

Default Value

******

API Name

jmx_passwd_file_readonly_user_password

Required

false

Name of User with Read-Write Access to the JMX Agent

Description

Specifies the name of the user that has read-write privileges when using password file based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

Default Value

controlRole

API Name

jmx_passwd_file_readwrite_user

Required

false

Password of user with read-write access to the JMX agent

Description

Specifies the password of the user that has read-write privileges when using password file based authentication for JMX access. JMX authentication must be enabled for this setting to take effect.

Related Name

Default Value

******

API Name

jmx_passwd_file_readwrite_user_password

Required

false

Maximum Client Connections

Description

The maximum number of concurrent connections (at the socket level) that a single client, identified by the IP address, may make to a single member of the ZooKeeper ensemble. This setting is used to prevent certain classes of DoS attacks, including file descriptor exhaustion. To remove the limit on concurrent connections, set this value to 0.

Related Name

maxClientCnxns

Default Value

60

API Name

maxClientCnxns

Required

false

Maximum Session Timeout

Description

The maximum session timeout, in milliseconds, that the ZooKeeper Server will allow the client to negotiate

Related Name

maxSessionTimeout

Default Value

40000

API Name

maxSessionTimeout

Required

false

Minimum Session Timeout

Description

The minimum session timeout, in milliseconds, that the ZooKeeper Server will allow the client to negotiate

Related Name

minSessionTimeout

Default Value

4000

API Name

minSessionTimeout

Required

false

ZooKeeper Server ID

Description

Unique identifier for each ZooKeeper server, typically starts at 1

Related Name

myid

Default Value

API Name

serverId

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Client Port

Description

The port to monitor for client connections. This is the port that clients attempt to connect to.

Related Name

clientPort

Default Value

2181

API Name

clientPort

Required

false

Election Port

Description

The port to monitor for leadership election

Related Name

Default Value

4181

API Name

electionPort

Required

false

Quorum Port

Description

The port to monitor for inter-server communication

Related Name

Default Value

3181

API Name

quorumPort

Required

false

JMX Remote Port

Description

The port used by the ZooKeeper Server's RMI registry. This is required to enable JMX access through RMI which is required for Cloudera Manager ZooKeeper monitoring. This is added as "-Dcom.sun.management.jmxremote.port" to the ZooKeeper Server's JVM command line.

Related Name

Default Value

9010

API Name

server_jmx_agent_port

Required

false

JMX RMI Server Port

Description

The port used by the ZooKeeper Server's RMI server to handle JMX RMI requests. This is added as "-Dcom.sun.management.jmxremote.rmi.port=*port*" to the ZooKeeper Server's JVM command line. This has an effect only in Oracle JDK 7u4 and higher. If the setting is left blank, the JMX Remote Port value is used. If set to 0 or -1, this setting is ignored. When this setting is not in effect, the JVM uses a random port for the RMI server.

Related Name

Default Value

API Name

server_jmx_rmi_port

Required

false

Admin Server Port

Description

Port number for the REST Admin Server embedded in ZooKeeper.

Related Name

admin.serverPort

Default Value

5181

API Name

zookeeper_admin_server_port

Required

false

Secure Client Port

Description

The port used in ZooKeeper to accept TLS/SSL connections from clients. You need to select 'Enable TLS/SSL for ZooKeeper' in order to have this port open. Any client that connects to this port must use TLS/SSL.

Related Name

secureClientPort

Default Value

2182

API Name

zookeeper_secure_client_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Java Heap Size of ZooKeeper Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

zookeeper_server_java_heapsize

Required

false

Security

Enable TLS client authentication for JMX port

Description

If enabled, a valid client certificate must be presented by the JMX client in order to connect to the JMX port. Ensure that the trusted CA certificates are present in either the ZooKeeper JMX TLS/SSL Server Trust Store File or the global trust store.

Related Name

Default Value

false

API Name

jmx_tls_client_auth_enabled

Required

false

Enable TLS/SSL for ZooKeeper JMX

Description

Encrypt communication between clients and ZooKeeper JMX using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

Default Value

false

API Name

jmx_tls_enabled

Required

false

ZooKeeper JMX TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when ZooKeeper JMX is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

Default Value

API Name

jmx_tls_keystore

Required

false

ZooKeeper JMX TLS/SSL Server Keystore File Password

Description

The password for the ZooKeeper JMX keystore file.

Related Name

Default Value

API Name

jmx_tls_keystore_password

Required

false

ZooKeeper JMX TLS/SSL Server Trust Store File

Description

The location on disk of the trust store, used to confirm the authenticity of TLS/SSL servers that ZooKeeper JMX might connect to. This is used when ZooKeeper JMX is the server in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

jmx_tls_truststore

Required

false

ZooKeeper JMX TLS/SSL Server Trust Store Password

Description

The password for the ZooKeeper JMX TLS/SSL Certificate Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

jmx_tls_truststore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: ZooKeeper 'Four Letter Word' Command Whitelist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper 'Four Letter Word' Command Whitelist parameter.

Related Name

Default Value

false

API Name

role_config_suppression_4lw_commands_whitelist

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Client Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_clientport

Required

true

Suppress Parameter Validation: Client Port Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Client Port Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_clientportaddress

Required

true

Suppress Parameter Validation: Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datadir

Required

true

Suppress Parameter Validation: Transaction Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Transaction Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_datalogdir

Required

true

Suppress Parameter Validation: Election Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Election Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_electionport

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Name of User with Read-Only access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with Read-Only access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readonly_user

Required

true

Suppress Parameter Validation: Password of User with Read-Only Access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of User with Read-Only Access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readonly_user_password

Required

true

Suppress Parameter Validation: Name of User with Read-Write Access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Name of User with Read-Write Access to the JMX Agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readwrite_user

Required

true

Suppress Parameter Validation: Password of user with read-write access to the JMX agent

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Password of user with read-write access to the JMX agent parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readwrite_user_password

Required

true

Suppress Parameter Validation: ZooKeeper JMX TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper JMX TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_keystore

Required

true

Suppress Parameter Validation: ZooKeeper JMX TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper JMX TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_keystore_password

Required

true

Suppress Parameter Validation: ZooKeeper JMX TLS/SSL Server Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper JMX TLS/SSL Server Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_truststore

Required

true

Suppress Parameter Validation: ZooKeeper JMX TLS/SSL Server Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper JMX TLS/SSL Server Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_truststore_password

Required

true

Suppress Parameter Validation: Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Quorum Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Quorum Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_quorumport

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: JMX Remote Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Remote Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_server_jmx_agent_port

Required

true

Suppress Parameter Validation: JMX RMI Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX RMI Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_server_jmx_rmi_port

Required

true

Suppress Parameter Validation: Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_server_role_env_safety_valve

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Java Configuration Options for Zookeeper Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Zookeeper Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zk_server_java_opts

Required

true

Suppress Parameter Validation: ZooKeeper Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zk_server_log_dir

Required

true

Suppress Parameter Validation: Admin Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Admin Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_admin_server_port

Required

true

Suppress Parameter Validation: Server Advanced Configuration Snippet (Safety Valve) for zoo.cfg

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server Advanced Configuration Snippet (Safety Valve) for zoo.cfg parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_config_safety_valve

Required

true

Suppress Parameter Validation: Secure Client Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Secure Client Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_secure_client_port

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_audit_health

Required

true

Suppress Health Test: Connection Count

Description

Whether to suppress the results of the Connection Count heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_connection_count

Required

true

Suppress Health Test: Data Directory Free Space

Description

Whether to suppress the results of the Data Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_data_directory_free_space

Required

true

Suppress Health Test: Transaction Log Directory Free Space

Description

Whether to suppress the results of the Transaction Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_data_log_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_log_directory_free_space

Required

true

Suppress Health Test: Maximum Request Latency

Description

Whether to suppress the results of the Maximum Request Latency heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_max_latency

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_otelcol_health

Required

true

Suppress Health Test: Outstanding Requests

Description

Whether to suppress the results of the Outstanding Requests heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_outstanding_requests

Required

true

Suppress Health Test: Quorum Membership

Description

Whether to suppress the results of the Quorum Membership heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_quorum_membership

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_zookeeper_server_unexpected_exits

Required

true

Service-Wide

Advanced

Auto Purge Time Interval

Description

The time interval in hours for which the purge task has to be triggered. Set to a positive integer (1 and above) to enable the auto purging. Defaults to 24.

Related Name

autopurge.purgeInterval

Default Value

1 day(s)

API Name

autopurgeInterval

Required

false

Auto Purge Snapshots Retain Count

Description

When enabled, ZooKeeper auto purge feature retains this many most recent snapshots and the corresponding transaction logs in the dataDir and dataLogDir respectively and deletes the rest. Defaults to 5. Minimum value is 3.

Related Name

autopurge.snapRetainCount

Default Value

5

API Name

autopurgeSnapRetainCount

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

zookeeper

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

zookeeper

API Name

process_username

Required

true

Enable auto-creation of data directories

Description

Automatically create data directories at startup, if they do not exist. Enabling this configuration should be used with care as it will suppress any errors in setup of data directories.

Related Name

Default Value

false

API Name

zookeeper_datadir_autocreate

Required

false

ZooKeeper Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

zookeeper_env_safety_valve

Required

false

Monitoring

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Log Event Retry Frequency

Description

The frequency in which the log4j event publication appender will retry sending undelivered log events to the Event server, in seconds

Related Name

Default Value

30

API Name

log_event_retry_frequency

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", "streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

ZooKeeper Canary Connection Timeout

Description

Configures the timeout used by the canary for connection establishment with ZooKeeper servers

Related Name

Default Value

10 second(s)

API Name

zookeeper_canary_connection_timeout

Required

false

ZooKeeper Canary Health Check

Description

Enables the health check that a client can connect to ZooKeeper and perform basic operations

Related Name

Default Value

true

API Name

zookeeper_canary_health_enabled

Required

false

ZooKeeper Canary Operation Timeout

Description

Configures the timeout used by the canary for ZooKeeper operations

Related Name

Default Value

30 second(s)

API Name

zookeeper_canary_operation_timeout

Required

false

ZooKeeper Canary Root Znode Path

Description

Configures the path of the root znode under which all canary updates are performed

Related Name

Default Value

/cloudera_manager_zookeeper_canary

API Name

zookeeper_canary_root_path

Required

false

ZooKeeper Canary Session Timeout

Description

Configures the timeout used by the canary sessions with ZooKeeper servers

Related Name

Default Value

30 second(s)

API Name

zookeeper_canary_session_timeout

Required

false

Healthy Server Monitoring Thresholds

Description

The health test thresholds of the overall Server health. The check returns "Concerning" health if the percentage of "Healthy" Servers falls below the warning threshold. The check is unhealthy if the total percentage of "Healthy" and "Concerning" Servers falls below the critical threshold.

Related Name

Default Value

Warning: 99.0 %, Critical: 51.0 %

API Name

zookeeper_servers_healthy_thresholds

Required

false

Other

Cleanup Retain Count

Description

The number of snapshot files and corresponding transaction logs to keep when running the Cleanup command.

Related Name

Default Value

5

API Name

cleanupRetainCount

Required

false

Initialization Limit

Description

Amount of time, in ticks, to allow followers to connect and sync to a leader. Increase this value as needed, if the amount of data managed by ZooKeeper is large.

Related Name

initLimit

Default Value

10

API Name

initLimit

Required

false

Jute Max Buffer

Description

The maximum size of the data that can be stored in a znode in bytes.

Related Name

jute.maxbuffer

Default Value

4 MiB

API Name

jute_maxbuffer

Required

false

Leader Serves

Description

Whether the leader accepts client connections.

Related Name

leaderServes

Default Value

yes

API Name

leaderServes

Required

false

Quorum Connection Manager Thread Pool Size

Description

Size of the thread pool quorum connection manager uses to manage connections between quorum servers. Only applies when ZooKeeper Server to Server SASL Authentication is enabled.

Related Name

quorum.cnxn.threads.size

Default Value

20

API Name

quorum_cnxn_threads_size

Required

false

Synchronization Limit

Description

Amount of time, in ticks, to allow followers to sync with ZooKeeper. If followers fall too far behind a leader, they are dropped.

Related Name

syncLimit

Default Value

5

API Name

syncLimit

Required

false

Tick Time

Description

The length of time, in milliseconds, of a single tick, which is the basic time unit used by ZooKeeper. A tick is used to regulate heartbeats and timeouts.

Related Name

tickTime

Default Value

2000

API Name

tickTime

Required

false

Security

Enable Kerberos Authentication

Description

Enable Kerberos authentication for ZooKeeper.

Related Name

enableSecurity

Default Value

false

API Name

enableSecurity

Required

false

Kerberos Principal

Description

Kerberos principal short name used by all roles of this service.

Related Name

Default Value

zookeeper

API Name

kerberos_princ_name

Required

true

Enable Server to Server SASL Authentication

Description

Enables SASL authentication between ZooKeeper servers. Only applies when ZooKeeper Kerberos Authentication is enabled.

Related Name

quorum.auth.enableSasl

Default Value

false

API Name

quorum_auth_enable_sasl

Required

false

Enable TLS/SSL for ZooKeeper

Description

Encrypt ZooKeeper communication using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)). This option will encrypt all internal communication between ZooKeeper servers (this feature is called QuorumSSL in ZooKeeper). Additionally, choosing this option will also encrypt the communication between ZooKeeper servers and all ZooKeeper client services that support TLS/SSL connections.

Related Name

zookeeper_tls_enabled

Default Value

false

API Name

zookeeper_tls_enabled

Required

false

ZooKeeper TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when ZooKeeper is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

zookeeper_tls_keystore

Default Value

API Name

zookeeper_tls_keystore

Required

false

ZooKeeper TLS/SSL Server Keystore File Password

Description

The password for the ZooKeeper keystore file.

Related Name

zookeeper_tls_keystore_password

Default Value

API Name

zookeeper_tls_keystore_password

Required

false

ZooKeeper TLS/SSL Server Trust Store File

Description

The location on disk of the trust store, used to confirm the authenticity of TLS/SSL servers that ZooKeeper might connect to. This is used when ZooKeeper is the server in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

zookeeper_tls_truststore

Default Value

API Name

zookeeper_tls_truststore

Required

false

ZooKeeper TLS/SSL Server Trust Store Password

Description

The password for the ZooKeeper TLS/SSL Certificate Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

zookeeper_tls_truststore_password

Default Value

API Name

zookeeper_tls_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: ZooKeeper 'Four Letter Word' Command Whitelist

Description

Whether to suppress configuration warnings produced by the ZooKeeper 'Four Letter Word' Command Whitelist configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_4lw_commands_whitelist

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Client Port

Description

Whether to suppress configuration warnings produced by the Client Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_clientport

Required

true

Suppress Configuration Validator: Client Port Address

Description

Whether to suppress configuration warnings produced by the Client Port Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_clientportaddress

Required

true

Suppress Configuration Validator: Data Directory

Description

Whether to suppress configuration warnings produced by the Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datadir

Required

true

Suppress Configuration Validator: Transaction Log Directory

Description

Whether to suppress configuration warnings produced by the Transaction Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_datalogdir

Required

true

Suppress Configuration Validator: Election Port

Description

Whether to suppress configuration warnings produced by the Election Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_electionport

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Name of User with Read-Only access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the Name of User with Read-Only access to the JMX Agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readonly_user

Required

true

Suppress Configuration Validator: Password of User with Read-Only Access to the JMX agent

Description

Whether to suppress configuration warnings produced by the Password of User with Read-Only Access to the JMX agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readonly_user_password

Required

true

Suppress Configuration Validator: Name of User with Read-Write Access to the JMX Agent

Description

Whether to suppress configuration warnings produced by the Name of User with Read-Write Access to the JMX Agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readwrite_user

Required

true

Suppress Configuration Validator: Password of user with read-write access to the JMX agent

Description

Whether to suppress configuration warnings produced by the Password of user with read-write access to the JMX agent configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_passwd_file_readwrite_user_password

Required

true

Suppress Configuration Validator: ZooKeeper JMX TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the ZooKeeper JMX TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_keystore

Required

true

Suppress Configuration Validator: ZooKeeper JMX TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the ZooKeeper JMX TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_keystore_password

Required

true

Suppress Configuration Validator: ZooKeeper JMX TLS/SSL Server Trust Store File

Description

Whether to suppress configuration warnings produced by the ZooKeeper JMX TLS/SSL Server Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_truststore

Required

true

Suppress Configuration Validator: ZooKeeper JMX TLS/SSL Server Trust Store Password

Description

Whether to suppress configuration warnings produced by the ZooKeeper JMX TLS/SSL Server Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_tls_truststore_password

Required

true

Suppress Configuration Validator: Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Server Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the Rules to Extract Events from Log Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: Quorum Port

Description

Whether to suppress configuration warnings produced by the Quorum Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_quorumport

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: JMX Remote Port

Description

Whether to suppress configuration warnings produced by the JMX Remote Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_server_jmx_agent_port

Required

true

Suppress Configuration Validator: JMX RMI Server Port

Description

Whether to suppress configuration warnings produced by the JMX RMI Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_server_jmx_rmi_port

Required

true

Suppress Configuration Validator: Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_server_role_env_safety_valve

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Java Configuration Options for Zookeeper Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Zookeeper Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zk_server_java_opts

Required

true

Suppress Configuration Validator: ZooKeeper Log Directory

Description

Whether to suppress configuration warnings produced by the ZooKeeper Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zk_server_log_dir

Required

true

Suppress Configuration Validator: Admin Server Port

Description

Whether to suppress configuration warnings produced by the Admin Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_admin_server_port

Required

true

Suppress Configuration Validator: Server Advanced Configuration Snippet (Safety Valve) for zoo.cfg

Description

Whether to suppress configuration warnings produced by the Server Advanced Configuration Snippet (Safety Valve) for zoo.cfg configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_config_safety_valve

Required

true

Suppress Configuration Validator: Secure Client Port

Description

Whether to suppress configuration warnings produced by the Secure Client Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_zookeeper_secure_client_port

Required

true

Suppress Parameter Validation: Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal parameter.

Related Name

Default Value

false

API Name

service_config_suppression_kerberos_princ_name

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Server Count Validator

Description

Whether to suppress configuration warnings produced by the Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_server_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: ZooKeeper Canary Root Znode Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Canary Root Znode Path parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_canary_root_path

Required

true

Suppress Parameter Validation: ZooKeeper Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_env_safety_valve

Required

true

Suppress Configuration Validator: ZooKeeper Server Count Validator

Description

Whether to suppress configuration warnings produced by the ZooKeeper Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_odd_number_of_servers_validator

Required

true

Suppress Configuration Validator: ZooKeeper Server-to-Server Authentication Validation

Description

Whether to suppress configuration warnings produced by the ZooKeeper Server-to-Server Authentication Validation configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_server_to_server_authentication_validator

Required

true

Suppress Parameter Validation: ZooKeeper TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_tls_keystore

Required

true

Suppress Parameter Validation: ZooKeeper TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_tls_keystore_password

Required

true

Suppress Parameter Validation: ZooKeeper TLS/SSL Server Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper TLS/SSL Server Trust Store File parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_tls_truststore

Required

true

Suppress Parameter Validation: ZooKeeper TLS/SSL Server Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ZooKeeper TLS/SSL Server Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_zookeeper_tls_truststore_password

Required

true

Suppress Health Test: ZooKeeper Canary

Description

Whether to suppress the results of the ZooKeeper Canary heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_zookeeper_canary_health

Required

true

Suppress Health Test: Server Health

Description

Whether to suppress the results of the Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_zookeeper_servers_healthy

Required

true

Host Configuration Properties

Advanced

P2P Parcel Distribution Port

Description

TCP port (on each cluster host) to be used for P2P Parcel Distribution. Set to 0 to disable P2P Parcel Distribution. This setting should only be modified when no parcels are being distributed.

Related Name

Default Value

7191

API Name

flood_torrent_port

Required

false

Cloudera Manager Agent Monitoring Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) used by Cloudera Manager Agent.

Related Name

Default Value

API Name

host_agent_safety_valve

Required

false

Java Home Directory

Description

Explicitly set the value of JAVA_HOME for all processes. This will override the auto-detection logic that is normally used.

Related Name

Default Value

API Name

java_home

Required

false

Data Services: Restrict workloads types

Description

Select Dedicated GPU Node for Machine Learning service when the host has Nvidia GPU.

- If Dedicated GPU Node is selected, this host will be reserved for workloads requiring GPU resources.
- Should only be used if this host has Nvidia GPU drivers installed.

Select Dedicated NVMe Node for Data Warehouse service when the host has NVMe for caching.

- If Dedicated NVMe Node is selected, this host will be reserved for workloads requiring NVMe resources.

Select None, if both are not applicable.

- This will be the default value.

These selections are applicable only for hosts that will be used in a Data Services Cluster. Certain workloads are scheduled to run on all nodes. If the taint was applied after CDP was installed, those workloads will not be drained from tainted nodes.

Related Name

Default Value

None

API Name

node_taint

Required

false

Host Upgrade Domain

Description

For advanced use only, the HDFS Upgrade Domain that a host belongs to. Only applies to DataNode hosts. Any DataNode hosts without an Upgrade Domain set will default to using the rack assignment of the host. This setting is not used if the Upgrade Domains block placement policy is not enabled for HDFS.

Related Name

upgrade_domain

Default Value

API Name

upgrade_domain

Required

false

Monitoring

Enable Health Alerts for This Host

Description

When set, Cloudera Manager will send alerts when the health of this host reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

false

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Cloudera Manager Agent TLS Certificate Expiry Thresholds

Description

The health test thresholds for monitoring the certificate of Cloudera Manager Agent.

Related Name

Default Value

Warning: 60 day(s), Critical: 7 day(s)

API Name

host_agent_certificate_expiry_thresholds

Required

false

Cloudera Manager Agent Log Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's log directory.

Related Name

Default Value

Warning: 2 GiB, Critical: 1 GiB

API Name

host_agent_log_directory_free_space_absolute_thresholds

Required

false

Cloudera Manager Agent Log Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

host_agent_log_directory_free_space_percentage_thresholds

Required

false

Cloudera Manager Agent Parcel Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's parcel directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

host_agent_parcel_directory_free_space_absolute_thresholds

Required

false

Cloudera Manager Agent Parcel Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's parcel directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Parcel Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

host_agent_parcel_directory_free_space_percentage_thresholds

Required

false

Cloudera Manager Agent Process Directory Free Space Monitoring Absolute Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's process directory.

Related Name

Default Value

Warning: 200 MiB, Critical: 100 MiB

API Name

host_agent_process_directory_free_space_absolute_thresholds

Required

false

Cloudera Manager Agent Process Directory Free Space Monitoring Percentage Thresholds

Description

The health check thresholds for monitoring of free space on the filesystem that contains the Cloudera Manager Agent's process directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Cloudera Manager Agent Process Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

host_agent_process_directory_free_space_percentage_thresholds

Required

false

Host Entropy Thresholds

Description

The health check thresholds for the available entropy on the host.

Related Name

Default Value

Warning: 100.0, Critical: 50.0

API Name

host_available_entropy_thresholds

Required

false

Host Clock Offset Thresholds

Description

The thresholds for the host clock offset health test. The test compares this threshold against the absolute value of the clock offset reported by the host's NTP service from the 'ntpdc -np' or 'chronyc sources' command. Setting both the warning and critical threshold values to never turns off collection of the clock offset by the Cloudera Manager Agent. If no time synchronization is in use, both threshold values should be set to never. Cloudera recommends using NTP for time synchronization of Hadoop clusters.

Related Name

Default Value

Warning: 3 second(s), Critical: 10 second(s)

API Name

host_clock_offset_thresholds

Required

false

Default Process Swap Memory Thresholds

Description

The default health test thresholds on the swap memory usage of the processes on the host. This value is used if process level threshold is equal to the default.

Related Name

Default Value

Warning: 200.0 page(s), Critical: Never

API Name

host_default_proc_memswap_thresholds

Required

false

Disk Device Collection Exclusion Regex

Description

The regular expression used to filter monitored disk devices and partitions. Disk device (for example, sda) and partition (for example, sda2) names that match this pattern will be excluded from metric collection.

Related Name

Default Value

^$

API Name

host_disk_collection_filter

Required

false

Host DNS Resolution Duration Thresholds

Description

The health check thresholds for the host DNS resolution duration.

Related Name

Default Value

Warning: 1 second(s), Critical: Never

API Name

host_dns_resolution_duration_thresholds

Required

false

Hostname and Canonical Name Health Check

Description

Whether the hostname and canonical names for this host are consistent when checked from a Java process.

Related Name

Default Value

true

API Name

host_dns_resolution_enabled

Required

false

Filesystem Check Error Exclusion Regex

Description

The regular expression used to filter filesystem check errors. Filesystem check errors that match this pattern will be put into debug log level.

Related Name

Default Value

^((/run/user/[0-9])|(/var/lib/kubernetes/*))

API Name

host_filesystem_check_error_filter

Required

false

Filesystem Collection Exclusion Regex

Description

The regular expression used to filter monitored filesystems. Mountpoints for filesystems (for example, /data/1) that match this pattern will be excluded from metric collection.

Related Name

Default Value

^$

API Name

host_fs_collection_filter

Required

false

Host Memory Swapping Thresholds

Description

The health test thresholds of the number of pages swapped out on the host in the last 15 minutes

Related Name

Default Value

Warning: 200.0 page(s), Critical: Never

API Name

host_memswap_thresholds

Required

false

Host Memory Swapping Check Window

Description

The amount of time over which the memory swapping test checks for pages swapped.

Related Name

Default Value

15 minute(s)

API Name

host_memswap_window

Required

false

Host Network Frame Error Test Minimum Required Packets

Description

The minimum number of received packets that must be received within the test window for this test to return "Bad" health. If less that this number of packets is received during the test window, the health check will never return "Bad" health.

Related Name

Default Value

0

API Name

host_network_frame_errors_floor

Required

false

Host Network Frame Error Percentage Thresholds

Description

The health check thresholds for the percentage of received packets that are frame errors.

Related Name

Default Value

Warning: Any, Critical: 0.5 %

API Name

host_network_frame_errors_thresholds

Required

false

Host Network Frame Error Check Window

Description

The amount of time over which the host frame error checks for frame errors.

Related Name

Default Value

15 minute(s)

API Name

host_network_frame_errors_window

Required

false

Network Interface Collection Exclusion Regex

Description

The regular expression used to filter monitored network interfaces. Network interfaces that match this pattern will be excluded from metric collection.

Related Name

Default Value

^(lo|bond[0-9]*)$

API Name

host_network_interface_collection_filter

Required

false

Host's Network Interfaces Slow Link Modes Thresholds

Description

The thresholds for the health check of the number of network interfaces that appear to be operating at less than full speed.

Related Name

Default Value

Warning: Any, Critical: Never

API Name

host_network_interfaces_slow_mode_thresholds

Required

false

Network Interface Expected Duplex Mode

Description

The expected duplex mode for network interfaces.

Related Name

Default Value

Full

API Name

host_nic_expected_duplex_mode

Required

false

Network Interface Expected Link Speed

Description

The expected network interface link speed.

Related Name

Default Value

1000

API Name

host_nic_expected_speed

Required

false

Host Process Health Test

Description

Enables the health test that the host's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

host_scm_health_enabled

Required

false

Host Triggers

Description

The configured triggers for this host. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific host.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if the host wait time exceeds 500 ms:[{"triggerName": "sample-trigger", "triggerExpression": "IF (select await_time where hostname= $HOSTNAME and last(await_time) > 500ms) DO health:concerning", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

host_triggers

Required

true

OpenTelemetry Collector Self Telemetry Section

Description

The OpenTelemetry Collector Self Telemetry provides information about its state for monitoring purposes. It requires a port where it publishes its metrics. This port will only be used if a role on the host requires OpenTelemetry Collector to run. See 'otelcol' related settings for services and roles. See the OpenTelemetry documentation.

Related Name

Default Value

telemetry: metrics: address: :8092

API Name

otelcol_telemetry

Required

false

Parcels

Parcel Directory

Description

The directory that parcels will be installed into on the host(s). The download 'parcel-cache' directory will be placed next to this directory on the filesystem. If the 'parcel_dir' variable is set in the Agent's config.ini file, it will override this value.

Related Name

Default Value

/opt/cloudera/parcels

API Name

parcels_directory

Required

true

Resource Management

Memory Overcommit Validation Threshold

Description

Threshold used when validating the allocation of RAM on a host. 0 means all of the memory is reserved for the system. 1 means none is reserved. Values can range from 0 to 1.

Related Name

Default Value

0.8

API Name

memory_overcommit_threshold

Required

false

Enable Cgroup-based Resource Management

Description

Enables resource management using control groups (cgroups). When toggled, roles on the host must be restarted for cgroups to be enabled or disabled. Per-resource controls are found in the configuration pages of role configuration groups and individual roles. Control groups are a feature of the Linux kernel, and support varies by distribution; see the Cloudera Manager documentation for details.

Related Name

Default Value

false

API Name

rm_enabled

Required

true

Suppressions

Suppress Configuration Validator: Cloudera Manager Agent User and Group Validator

Description

Whether to suppress configuration warnings produced by the Cloudera Manager Agent User and Group Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_agent_system_user_group_validator

Required

true

Suppress Configuration Validator: CGroups Disabled Validator

Description

Whether to suppress configuration warnings produced by the CGroups Disabled Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_cgroups_disabled_validator

Required

true

Suppress Parameter Validation: P2P Parcel Distribution Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the P2P Parcel Distribution Port parameter.

Related Name

Default Value

false

API Name

host_config_suppression_flood_torrent_port

Required

true

Suppress Parameter Validation: Cloudera Manager Agent Monitoring Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Agent Monitoring Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_agent_safety_valve

Required

true

Suppress Parameter Validation: Disk Device Collection Exclusion Regex

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Disk Device Collection Exclusion Regex parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_disk_collection_filter

Required

true

Suppress Parameter Validation: Filesystem Check Error Exclusion Regex

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Filesystem Check Error Exclusion Regex parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_filesystem_check_error_filter

Required

true

Suppress Parameter Validation: Filesystem Collection Exclusion Regex

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Filesystem Collection Exclusion Regex parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_fs_collection_filter

Required

true

Suppress Parameter Validation: Network Interface Collection Exclusion Regex

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Network Interface Collection Exclusion Regex parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_network_interface_collection_filter

Required

true

Suppress Parameter Validation: Host Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Triggers parameter.

Related Name

Default Value

false

API Name

host_config_suppression_host_triggers

Required

true

Suppress Parameter Validation: Java Home Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Home Directory parameter.

Related Name

Default Value

false

API Name

host_config_suppression_java_home

Required

true

Suppress Configuration Validator: Java Version Validator

Description

Whether to suppress configuration warnings produced by the Java Version Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_java_version_required_for_cdh_validator

Required

true

Suppress Configuration Validator: Memory Overcommited Validator

Description

Whether to suppress configuration warnings produced by the Memory Overcommited Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_memory_overcommitted_validator

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Self Telemetry Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Self Telemetry Section parameter.

Related Name

Default Value

false

API Name

host_config_suppression_otelcol_telemetry

Required

true

Suppress Parameter Validation: Parcel Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Parcel Directory parameter.

Related Name

Default Value

false

API Name

host_config_suppression_parcels_directory

Required

true

Suppress Configuration Validator: Rack Diversity Validator

Description

Whether to suppress configuration warnings produced by the Rack Diversity Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_rack_diversity_validator

Required

true

Suppress Configuration Validator: Supervisord Version Validator

Description

Whether to suppress configuration warnings produced by the Supervisord Version Validator configuration validator.

Related Name

Default Value

false

API Name

host_config_suppression_supervisord_version_matched_with_cm_validator

Required

true

Suppress Parameter Validation: Host Upgrade Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Upgrade Domain parameter.

Related Name

Default Value

false

API Name

host_config_suppression_upgrade_domain

Required

true

Suppress Health Test: Certificate Expiration

Description

Whether to suppress the results of the Certificate Expiration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_agent_certificate_expiry

Required

true

Suppress Health Test: Agent Log Directory

Description

Whether to suppress the results of the Agent Log Directory heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_agent_log_directory_free_space

Required

true

Suppress Health Test: Agent Parcel Directory

Description

Whether to suppress the results of the Agent Parcel Directory heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_agent_parcel_directory_free_space

Required

true

Suppress Health Test: Agent Process Directory

Description

Whether to suppress the results of the Agent Process Directory heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_agent_process_directory_free_space

Required

true

Suppress Health Test: Entropy

Description

Whether to suppress the results of the Entropy heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_available_entropy

Required

true

Suppress Health Test: Clock Offset

Description

Whether to suppress the results of the Clock Offset heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_clock_offset

Required

true

Suppress Health Test: DNS Resolution

Description

Whether to suppress the results of the DNS Resolution heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_dns_resolution

Required

true

Suppress Health Test: Swapping

Description

Whether to suppress the results of the Swapping heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_memory_swapping

Required

true

Suppress Health Test: Frame Errors

Description

Whether to suppress the results of the Frame Errors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_network_frame_errors

Required

true

Suppress Health Test: Network Interface Speed

Description

Whether to suppress the results of the Network Interface Speed heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_network_interfaces_slow_mode

Required

true

Suppress Health Test: Agent Status

Description

Whether to suppress the results of the Agent Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

host_health_suppression_host_scm_health

Required

true

Cloudera Manager Server Properties

Advanced

Command Eviction Age

Description

Length of time after which inactive commands are evicted from the database. Default is two years.

Related Name

Default Value

730 day(s)

API Name

command_eviction_age_hours

Required

true

Cloudera Manager Server Local Data Storage Directory

Description

Local path used by Cloudera Manager for storing data, including command result files. Note that changes to this configuration will only apply to commands started after the change. It is highly recommended that existing data be migrated over to the new location for the data to be accessible via and managed by Cloudera Manager.

Related Name

Default Value

/var/lib/cloudera-scm-server

API Name

command_storage_path

Required

false

Cloudera Manager Agent Connections Disabled Protocols

Description

List of Disabled Protocols for Cloudera Manager Server to Cloudera Manager Agent HTTP/HTTPS Connections

Related Name

Default Value

API Name

disabled_agent_connection_protocols

Required

false

Enable Debugging of API

Description

When enabled, the server log will contain traces of all API calls.

Related Name

Default Value

false

API Name

enable_api_debug

Required

true

Extra JVM arguments for Java-based services

Description

A list of extra JVM arguments that Cloudera Manager will append to the command line for Java-based services.

Related Name

Default Value

API Name

extra_jvm_opts

Required

false

Agent Heartbeat Logging Directory

Description

Specifies the location where Agent heartbeat requests and responses should be logged, for debugging purposes. If empty, logging is disabled.

Related Name

Default Value

API Name

heartbeat_logging_dir

Required

false

Offline Command Timeout

Description

The amount of time (in seconds) to wait for all requested hosts to be offlined. If all requested hosts are not transitioned to offline in this interval, the command fails. If timeout occurs, hosts that transitioned to maintenance stay in maintenance, and those that failed to transition are returned to the normal state.

Related Name

Default Value

10 minute(s)

API Name

offline_default_timeout

Required

false

Queue Manager Request Timeout

Description

Timeout for the Management console to fetch resources related to the YARN Queue Manager. This value may need to be increased for larger deployments where the Management console times out trying to fetch resources from the YARN Queue Manager.

Related Name

scm.server.qm_proxy.timeout

Default Value

5 minute(s)

API Name

qm_proxy_timeout

Required

true

Cloudera Manager Descriptor Fetch Timeout

Description

Timeout for Cloudera Management Service roles to fetch deployment descriptor from Cloudera Manager service. This may need to be increased for larger deployments where Management roles are timing out trying to fetch the descriptor.

Related Name

scm.server.proxy.timeout

Default Value

10 second(s)

API Name

scm_proxy_timeout

Required

true

Tags Limit

Description

The maximum number of tags that can be created globally. Note that creating more tags than are allowed by the default limit may lead to decreased performance of Cloudera Manager.

Related Name

Default Value

100000

API Name

tags_limit

Required

false

Maximum Number of Time-Series Streams Returned Per Heatmap

Description

The maximum number of time-series streams returned by a single time-series heatmap query. The default is 10,000 streams. This value can be set higher, but increasing it may negatively impact chart performance and may require more resources be given to the Cloudera Manager Server, Host Monitor, and Service Monitor.

Related Name

Default Value

10000

API Name

tsquery_heatmap_streams_limit

Required

true

Time-Series Request Timeout

Description

Timeout for requests to Service and Host Monitor.

Related Name

Default Value

20 second(s)

API Name

tsquery_request_timeout

Required

true

Maximum Number of Time-Series Streams Returned Per Scatter Plot

Description

The maximum number of time-series streams returned by a single time-series scatter plot. The default is 1000 streams. This value can be set higher, but increasing it may negatively impact chart performance and may require more resources be given to the Cloudera Manager Server, Host Monitor, and Service Monitor.

Related Name

Default Value

1000

API Name

tsquery_scatter_streams_limit

Required

true

Maximum Number Of Time-Series Streams Returned Per Line-Based Chart

Description

The maximum number of time-series streams that will be returned by a single time-series query. The default is 250 streams. This value can be set higher, but increasing it may negatively impact

chart performance and may require more resources be given to the Cloudera Manager Server, Host Monitor, and Service Monitor.

Related Name

Default Value

250

API Name

tsquery_streams_limit

Required

true

Maximum Number of Time-Series Streams Returned Per Table

Description

The maximum number of time-series streams returned in a single time-series table. The default is 2000 streams. This value can be set higher, but increasing it may negatively impact chart performance and may require more resources be given to the Cloudera Manager Server, Host Monitor, and Service Monitor.

Related Name

Default Value

2000

API Name

tsquery_table_streams_limit

Required

true

Altus

Telemetry Altus Account

Description

The account to use for data collection to Altus. This by itself does not enable telemetry. Telemetry needs to be explicitly enabled for specific services.

Related Name

Default Value

API Name

telemetry_altus_account

Required

false

Custom Service Descriptors

Enable Local Descriptor Repository

Description

When enabled, the server will read custom service descriptors from the local filesystem.

Related Name

Default Value

true

API Name

csd_repo_enabled

Required

true

Local Descriptor Repository Path

Description

Path to the local repository where custom service descriptors are located.

Related Name

Default Value

/opt/cloudera/csd

API Name

csd_repo_path

Required

true

External Authentication

Authentication Backend Order

Description

The order in which authentication back ends are used for authenticating a user. Emergency Administrator Access allows Full and User Administrators in the local database to authenticate if external authentication is not functioning.

Related Name

Default Value

DB_ONLY

API Name

auth_backend_order

Required

true

External Authentication Program Path

Description

An external script (or binary) to use to authenticate users. Username is passed as the first command line argument. The password is passed over stdin. You can configure the return codes for the external script on the Roles page. A negative return value indicates a failure. A failure description can be printed to stderr.

Related Name

Default Value

API Name

auth_script

Required

false

Authorization Backend Order.

Description

The order in which authorization back ends are used for authorizing a user.This determines where a user's roles come from. If "Database and External" is chosen, then the union of all roles is used.

Related Name

Default Value

EXTERNAL_AND_DB

API Name

authorization_backend_order

Required

true

Enable SPNEGO/Kerberos Authentication for the Admin Console and API

Description

When enabled, you can authenticate to the Cloudera Manager Admin Console and API using Kerberos via the SPNEGO protocol. If you have not imported Kerberos admin credentials, you must also specify the Kerberos principal for SPNEGO authentication and Kerberos keytab file for SPNEGO authentication. This method of authentication is in addition to the configured external authentication methods.

Related Name

Default Value

false

API Name

krb_auth_enable

Required

true

Exclude Users for SPNEGO/Kerberos Authentication

Description

Users in this list will not be allowed to authenticate to Cloudera Manager using SPNEGO/Kerberos. They can still authenticate using other methods.

Related Name

Default Value

admin

API Name

krb_auth_exclude_users

Required

false

Keytab File for SPNEGO Authentication Override

Description

This is a path to the keytab file that Cloudera Manager will use for SPNEGO/Kerberos authentication. You can leave this blank to have Cloudera Manager automatically generate this keytab.

Related Name

Default Value

API Name

krb_auth_keytab

Required

false

Kerberos Principal for SPNEGO Authentication Override

Description

This is the full name of the service principal that Cloudera Manager will use for SPNEGO/Kerberos authentication. It is usually "HTTP/fqdn@REALM" where "fqdn" is the Cloudera Manager host and "REALM" is the Kerberos domain. The Kerberos keytab file for SPNEGO authentication must contain an entry for this principal. You can leave this blank to have Cloudera Manager automatically generate this principal.

Related Name

Default Value

API Name

krb_auth_principal

Required

false

LDAP Bind User Distinguished Name

Description

Distinguished name of the user to bind to AD as for user authentication search/bind and group lookup for role authorization. For openLDAP based directories this should be a DN string, for Active Directory this can be just a username, combined with the "Active Directory Domain" value for login. For example username in the field and example.com in the active directory domain will result in the User Principal Name value of username@example.com being used to bind. If you put a UPM value here, do not over-configure the "active directory domain" field otherwise you will end up presenting username@example.com@example.com for binds. AD will accept a UPN value or the DN value as a valid Bind DN; An example of a Distinguished Name (DN): CN=cdh admin,OU=svcaccount,DC=example,DC=com An example of a UPN value: cdhadmin@example.com

Related Name

Default Value

API Name

ldap_bind_dn

Required

false

LDAP Bind Password

Description

The password of the bind user.

Related Name

Default Value

API Name

ldap_bind_pw

Required

false

LDAP Distinguished Name Pattern

Description

This setting is deprecated and soon to be removed, do not use LDAP Distinguished Name Pattern for configuration moving forward. It is not necessary to use and deprecated as a configuration approach for LDAP and AD in general.

Related Name

Default Value

API Name

ldap_dn_pattern

Required

false

LDAP Group Search Base

Description

The distinguished name indicating the path within the directory information tree to begin user searches from. For example in AD it would be cn=groups,dc=example,dc=com. Or in an openLDAP compatible situation it would be something like ou=groups,dc=example,dc=com. Check with your directory administration team on the proper search base to configure for your environment.

Related Name

Default Value

API Name

ldap_group_search_base

Required

false

LDAP Group Search Filter

Description

The search filter to use for finding groups for authorization of authenticated users for their Cloudera Manager role. For Active Directory and openLDAP compatible directories this will usually be (member={0}), where {0} will be replaced by DN string for a successfully authenticated user through the search/bind process. This requires configuration of the LDAP Bind User Distinguished Name field.

Related Name

Default Value

API Name

ldap_group_search_filter

Required

false

External Authentication Type

Description

The type of external authentication to use.

Related Name

Default Value

ACTIVE_DIRECTORY

API Name

ldap_type

Required

true

LDAP URL

Description

The URL of the LDAP server. The URL must be prefixed with ldap:// or ldaps://. The URL can optionally specify a custom port, for example: ldaps://ldap_server.example.com:1636. Note that usernames and passwords will be transmitted in the clear unless either an ldaps:// URL is used, or "Enable LDAP TLS" is turned on (where available). Also note that encryption must be in use between the client and this service for the same reason.For more detail on the LDAP URL format, see RFC 2255

Related Name

Default Value

API Name

ldap_url

Required

false

LDAP User Search Base

Description

The distinguished name indicating the path within the directory information tree to begin user searches from. For example in AD it would be cn=users,dc=example,dc=com. Or in an openLDAP compatible situation it would be something like ou=people,dc=example,dc=com. Check with your directory administration team on the proper user search base to configure for your environment.

Related Name

Default Value

API Name

ldap_user_search_base

Required

false

LDAP User Search Filter

Description

The search filter to use for finding users. For AD configuration it will be (sAMAccountName={0}) and for openLDAP compatible directories it will usually be (uid={0}). Note that a custom attribute can also be used if the directory is configured differently for user names. The {0} expands the currently authenticating user"s name entered in the login form for the query.

Related Name

Default Value

API Name

ldap_user_search_filter

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

Default Value

API Name

nt_domain

Required

false

PAM Service Name

Description

The service name that identifies the PAM module used to verify the username and password. This is typically the name of a file under /etc/pam.d/ on the Cloudera Manager server host.

Related Name

Default Value

login

API Name

pam_service_name

Required

false

Allowed Groups for Knox Proxy

Description

When Apache Knox makes a proxy request to Cloudera Manager, the proxied user must belong to one of these LDAP groups. This configuration is only used if LDAP authentication is enabled and the Authorization Backend Order is not Database Only. A wildcard "*" entry allows any group.

Related Name

Default Value

API Name

proxyuser_knox_groups

Required

false

Allowed Hosts for Knox Proxy

Description

When Apache Knox makes a proxy request to Cloudera Manager, the request must come from one of these hosts. You can specify either an IP address or a fully-qualified domain name. If using multiple Knox gateways, make sure that all gateway hosts are listed here. A wildcard "*" entry allows any host.

Related Name

Default Value

API Name

proxyuser_knox_hosts

Required

false

Knox Proxy Principal

Description

This is the service name of the Kerberos principal that Apache Knox will use to authenticate to Cloudera Manager when making proxy requests. Usually, this should be set to "knox" when using Knox to proxy to Cloudera Manager. If empty, Cloudera Manager will not accept proxy requests from any principal. The service name does not have to be a valid user.

Related Name

Default Value

knox

API Name

proxyuser_knox_principal

Required

false

Allowed Users for Knox Proxy

Description

When Apache Knox makes a proxy request to Cloudera Manager, the proxied user must be one of these users. A wildcard "*" entry allows any user.

Related Name

Default Value

API Name

proxyuser_knox_users

Required

false

SAML Entity Alias

Description

Unique alias used to identify the selected instance of local service provider based on used URL.

Related Name

Default Value

clouderaManager

API Name

saml_entity_alias

Required

false

SAML Entity Base URL

Description

The Base URL used to construct redirect URLs reported in this server's SP metadata. Leave this blank to let the server calculate the base URL itself.

Related Name

Default Value

API Name

saml_entity_base_url

Required

false

SAML Entity ID

Description

The ID that Cloudera Manager will use to identify itself to the IDP. This value should be unique to this Cloudera Manager installation.

Related Name

Default Value

clouderaManager

API Name

saml_entity_id

Required

true

Alias of SAML Sign/Encrypt Private Key

Description

The alias used to identify the sign/encrypt private key in the SAML keystore.

Related Name

Default Value

API Name

saml_key_alias

Required

false

SAML Sign/Encrypt Private Key Password

Description

The password for the sign/encrypt private key in the SAML keystore.

Related Name

Default Value

API Name

saml_key_password

Required

false

SAML Keystore Password

Description

The password for the SAML keystore.

Related Name

Default Value

API Name

saml_keystore_password

Required

false

Path to SAML Keystore File

Description

The filesystem path to the keystore file containing the SP private key and any necessary public certificates to validate the IDP.

Related Name

Default Value

API Name

saml_keystore_path

Required

false

SAML Login URL

Description

If your IDP does not support SP-initiated SSO (very uncommon), you use a separate login URL, outside of Cloudera Manager. Provide that URL here so that Cloudera Manager can use it when a user needs to log in.

Related Name

Default Value

API Name

saml_login_url

Required

false

Path to SAML IDP Metadata File

Description

The filesystem path to the IDP metadata XML file.

Related Name

Default Value

API Name

saml_metadata_path

Required

false

SAML Attribute Identifier for User Role

Description

The URN OID that will identify the user's role in the SAML attributes. Only has an effect when 'Attribute' based role assignment is used.

Related Name

Default Value

urn:oid:2.5.4.11

API Name

saml_oid_role

Required

true

SAML Attribute Identifier for User ID

Description

The URN OID that will identify the user's ID in the SAML attributes.

Related Name

Default Value

urn:oid:0.9.2342.19200300.100.1.1

API Name

saml_oid_user

Required

true

SAML Response Binding

Description

The SAML Binding format that the IDP is asked to use when sending authentication responses.

Related Name

Default Value

ARTIFACT

API Name

saml_response_binding

Required

true

SAML Role Assignment Mechanism

Description

The mechanism to use for assigning roles to users. 'Attribute' assigns roles based on a SAML attribute. 'Script' assigns roles based on the result of an external script.

Related Name

Default Value

ATTRIBUTE

API Name

saml_role_mapper

Required

true

Path to SAML Role Assignment Script

Description

An external script (or binary) to use to assign roles to SAML users. The username is passed as the first command-line argument. You can configure the return codes for the external script on the Roles page. A negative return value indicates a failure.

Related Name

Default Value

API Name

saml_role_script

Required

false

SAML Message Signing Algorithm

Description

Sets the signing algorithm to use when signing the SAML messages.

Related Name

Default Value

RSA_SHA512

API Name

saml_signature_algo

Required

false

SAML Single Logout (SLO)

Description

When enabled, Cloudera Manager sends a Single Logout (SLO) request to the Identity Provider (IdP).

Related Name

Default Value

false

API Name

saml_slo

Required

true

Source of User ID in SAML Response

Description

Whether the user ID should be obtained from the SAML response's NameID field or from an attribute

Related Name

Default Value

ATTRIBUTE

API Name

saml_user_source

Required

true

Kerberos

Active Directory Account Prefix

Description

Prefix used in names while creating accounts in Active Directory. The prefix can be up to 15 characters long and can be set to identify accounts used for authentication by CDH processes. Used only if Active Directory KDC is used for authentication.

Related Name

Default Value

API Name

ad_account_prefix

Required

false

Active Directory Account Properties

Description

Active Directory account properties used in credential generation. Used only if Active Directory KDC is being used for authentication. Only accountExpires is supported.

Related Name

Default Value

accountExpires=0, objectClass=top, objectClass=person, objectClass=organizationalPerson, objectClass=user

API Name

ad_account_properties

Required

false

Active Directory Delete Accounts on Credential Regeneration

Description

Set this option to true if regeneration of credentials should automatically delete the associated Active Directory accounts. Used only if Active Directory KDC is used for authentication.

Related Name

Default Value

false

API Name

ad_delete_on_regenerate

Required

false

Active Directory Suffix

Description

Active Directory suffix where all the accounts used by CDH daemons will be created. Used only if Active Directory KDC is being used for authentication.

Related Name

Default Value

ou=hadoop, DC=hadoop, DC=com

API Name

ad_kdc_domain

Required

true

Active Directory LDAP Port

Description

Port to use for LDAP when using Active Directory for authentication. This port is going to transmit encrypted information protected by Kerberos SASL.

Related Name

Default Value

389

API Name

ad_ldap_port

Required

true

Active Directory LDAPS Port

Description

Port to use for LDAP over TLS/SSL when using Active Directory for authentication.

Related Name

Default Value

636

API Name

ad_ldaps_port

Required

true

Active Directory Password Properties

Description

Active Directory password properties used in password generation. Used only if Active Directory KDC is being used for authentication.

Related Name

Default Value

length=12, minLowerCaseLetters=2, minUpperCaseLetters=2, minDigits=2, minSpaces=0, minSpecialChars=0, specialChars=?.!$%^*()-_+=~

API Name

ad_password_properties

Required

false

Active Directory Set Encryption Types

Description

Set this option to true if creation of Active Directory accounts should automatically turn on the associated encryption types represented by the msDS-EncryptionTypes field. Used only if Active Directory KDC is used for authentication.

Related Name

Default Value

false

API Name

ad_set_encryption_types

Required

false

Custom Kerberos Keytab Retrieval Script

Description

Specify the path to a custom script (or executable) to retrieve a Kerberos keytab. The script should take two arguments: a destination file to write the keytab to, and the full principal name to retrieve the key for. If this property is specified, Cloudera Manager ignores all other properties specified for Kerberos setup.

Related Name

Default Value

API Name

gen_keytab_script

Required

false

Active Directory Domain Controller Override

Description

If multiple Active Directory Domain Controllers are behind a load-balancer, Cloudera Manager should be provided with the address of one of them. Cloudera Manager then sends commands to create accounts to that Domain Controller only. Note: This setting is used only while creating accounts. CDH services use the value entered in the KDC Server Host field only while authenticating.

Related Name

Default Value

API Name

kdc_account_creation_host_override

Required

false

KDC Admin Server Host

Description

Host where the KDC Admin server is located. Port number is optional and can be provided as hostname[:port]

Related Name

admin_server

Default Value

API Name

kdc_admin_host

Required

false

KDC Server Host

Description

Host where the KDC server is located. Port number is optional and can be provided as hostname[:port]

Related Name

kdc

Default Value

API Name

kdc_host

Required

false

KDC Type

Description

Type of KDC used for authentication in CDH clusters

Related Name

Default Value

MIT KDC

API Name

kdc_type

Required

true

DNS Lookup KDC

Description

Indicate whether DNS SRV records should be used to locate the KDCs and other servers for a realm, if they are not listed in the krb5.conf information for the realm.

Related Name

dns_lookup_kdc

Default Value

false

API Name

krb_dns_lookup_kdc

Required

true

Domain Name(s)

Description

Domain(s) which are mapped to this Kerberos Realm. This is used to generate [domain_realm] section. Also, the first domain is used as default_domain in [realms] section

Related Name

Default Value

API Name

krb_domain

Required

false

Kerberos Encryption Types

Description

Encryption types supported by KDC. Note: To use AES encryption, make sure you have deployed JCE Unlimited Strength Policy File by following the instructions here.

Related Name

Default Value

rc4-hmac

API Name

krb_enc_types

Required

false

Forwardable Tickets

Description

If this flag is true, initial tickets will be forwardable by default, if allowed by the KDC.

Related Name

forwardable

Default Value

true

API Name

krb_forwardable

Required

true

KDC Timeout

Description

The maximum time to wait for a reply from the KDC. A time of 0 seconds means "use the client's default".

Related Name

kdc_timeout

Default Value

3 second(s)

API Name

krb_kdc_timeout

Required

false

krb5.conf file path

Description

Set the path to the krb5.conf file for all Cloudera processes. This is a required field with a default value of '/etc/krb5.conf'. If the option 'Manage krb5.conf through Cloudera Manager' is not selected, you must copy the /etc/krb5.conf file to all cluster hosts. Note: If you configure a non-default file path (default path is /etc/krb5.conf) the KDC services must be configured by your system administrator. Also, check the documentation to add the new krb5.conf path to Cloudera Manager Server to avoid KDC health check failures.

Related Name

Default Value

/etc/krb5.conf

API Name

krb_krb5_conf_path

Required

true

Advanced Configuration Snippet (Safety Valve) for [libdefaults] section of krb5.conf

Description

For advanced use only. Any text here will be emitted verbatim in the [libdefaults] section of krb5.conf.

Related Name

Default Value

API Name

krb_libdefaults_safety_valve

Required

false

Manage krb5.conf through Cloudera Manager

Description

Whether Cloudera Manager should configure and deploy krb5.conf on secure clusters. If this option is not selected, then you must ensure that krb5.conf is deployed on all hosts in a secure cluster, including the Cloudera Manager Server host. Note: If you configure a non-default file path (default path is /etc/krb5.conf) the KDC services must be configured by your system administrator. Also, check the documentation to add the new krb5.conf path to Cloudera Manager Server to avoid KDC health check failures.

Related Name

Default Value

false

API Name

krb_manage_krb5_conf

Required

false

Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf

Description

For advanced use only. Cloudera Manager configures the [libdefaults], [realms] and [domain_realm] section of krb5.conf. Any text here will be emitted verbatim after them in krb5.conf.

Related Name

Default Value

API Name

krb_other_safety_valve

Required

false

Advanced Configuration Snippet (Safety Valve) for the Default Realm in krb5.conf

Description

For advanced use only. Any text here will be emitted verbatim in the [realms] section of krb5.conf for the specified security realm. If you want to add realms besides the default one, configure them using Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf.

Related Name

Default Value

API Name

krb_realms_safety_valve

Required

false

Kerberos Renewable Lifetime

Description

Default renewable lifetime for initial ticket requests.

Related Name

renew_lifetime

Default Value

7 day(s)

API Name

krb_renew_lifetime

Required

true

Kerberos Ticket Lifetime

Description

Default lifetime for initial ticket requests.

Related Name

ticket_lifetime

Default Value

1 day(s)

API Name

krb_ticket_lifetime

Required

true

Maximum Renewable Life for Principals

Description

Maximum renewable lifetime for Kerberos principals generated by Cloudera Manager. This property is used only if MIT KDC is used. Set this property to zero if the KDC should provide the maximum renewable lifetime. Note: Principals with non-renewable tickets are not recommended because they can prevent Hadoop services from functioning.

Related Name

Default Value

5 day(s)

API Name

max_renew_life

Required

true

Kerberos Security Realm

Description

The realm to use for Kerberos security. Note: Changing this setting would clear up all existing credentials and keytabs from Cloudera Manager.

Related Name

default_realm

Default Value

HADOOP.COM

API Name

security_realm

Required

true

Kerberos Trusted Realms

Description

List of Kerberos realms that all services on this Cloudera Manager should trust. This parameter is used to configure and verify krb5.conf file. The parameter is auto-configured while adding a peer, but it is recommended that users ensure the values are correct.

Related Name

trusted_realms

Default Value

API Name

trusted_realms

Required

false

Monitoring

Cross Entity Aggregate Generation Filters

Description

Specifies two filters, a blacklist and a whitelist, that impact cross-entity aggregates generated by the Cloudera Manager monitoring system. By default, cross-entity aggregates are generated for all types. The blacklist entries can be used to disable generation of cross-entity aggregates, and whitelist entries can be used to force their creation.The JSON structure of this field is as follows:

- blacklist - A filter that when matched will prevent cross-entity aggregate creation. The structure of the filter is outlined below.
- whitelist - A filter that when matched will force cross-entity aggregate creation. The structure of the filter is outlined below. This filter takes precedence over the blacklist filter, so if both are matched, an aggregate will be generated.

The JSON structure of either filter is as follows:

- types - A list of entries in the following format sourceType::targetType::aggregateMetricType, e.g. DATANODE::RACK::STATISTICAL.
- streams - A list of entries in the following format sourceType::targetType::metricName::aggregateMetricType, e.g. HOST::CLUSTER::fd_open::TOTAL.

In the above filters the source and target types are entity type strings used within the metric system. ROLE, SERVICE and ALL are wildcards that match all role types, service types and all types respectively. Metrics are referred to by their user facing names, so counter-based metrics will be in _rate form. The two types of aggregate metrics are TOTAL and STATISTICAL.After making changes to this field, both the Cloudera Manager Server and the Service and Host Monitors should be restarted.For advanced use only. You could break Cloudera Manager charting and health functionality by editing this field.

Related Name

Default Value

blacklist: streams : [ ], types : [KUDU_REPLICA::KUDU_TABLET::STATISTICAL] , whitelist: streams : [ ], types : [ ]

API Name

cross_entity_aggregate_filters

Required

false

Set health status to Bad if the Agent heartbeats fail

Description

If an Agent fails to send this number of expected consecutive heartbeats to the Server, a "Bad" health status is assigned to that Agent.

Related Name

Default Value

10 time(s)

API Name

missed_hb_bad

Required

true

Set health status to Concerning if the Agent heartbeats fail

Description

If an Agent fails to send this number of expected consecutive heartbeats to the Server, a "Concerning" health status is assigned to that Agent.

Related Name

Default Value

5 time(s)

API Name

missed_hb_concerning

Required

true

Network

No Proxy List

Description

The no proxy list setting to include comma separated list of Cloudera specific names or IP addresses to avoid internal traffic routing through the Internet, also supports wildcard values e.g. "*.cloudera.site, localhost, 172.0.0.1, 169.254.169.254, 170.254.169.254, 169.254.169.255".

Related Name

Default Value

API Name

parcel_no_proxy_list

Required

false

Proxy Password

Description

The basic authentication password for the proxy.

Related Name

Default Value

API Name

parcel_proxy_password

Required

false

Proxy Port

Description

The port for the proxy server to be used when the Cloudera Manager Server accesses the Internet, such as when downloading parcels and uploading diagnostic data.

Related Name

Default Value

API Name

parcel_proxy_port

Required

false

Proxy Protocol

Description

The protocol to use for the proxy server when the Cloudera Manager Server accesses the Internet, such as when downloading parcels and uploading diagnostic data.

Related Name

Default Value

HTTP

API Name

parcel_proxy_protocol

Required

true

Proxy Server

Description

The proxy server to be used when the Cloudera Manager Server accesses the Internet, such as when downloading parcels and uploading diagnostic data.

Related Name

Default Value

API Name

parcel_proxy_server

Required

false

Proxy User

Description

The basic authentication user name for the proxy.

Related Name

Default Value

API Name

parcel_proxy_user

Required

false

Enable Automatic Authentication for Cloudera Repositories

Description

You must enable this option if you are accessing Cloudera Repositories that require authentication. Cloudera Manager will use the configured HTTP authentication override username and password

if configured, or the information from the installed license. You can disable this option if you are using local repository mirrors, if you have an internal alias or mirror to archive.cloudera.com, or if you are only using the public Cloudera Repositories that do not require authentication.

Related Name

Default Value

true

API Name

remote_repo_auth

Required

false

HTTP authentication password override for Cloudera Repositories

Description

Use this only in consultation with Cloudera Support. Specify an override password for HTTP authentication for Cloudera Repositories. You must also specify HTTP authentication override username.

Related Name

Default Value

API Name

remote_repo_override_password

Required

false

HTTP authentication username override for Cloudera Repositories

Description

Use this only in consultation with Cloudera Support. Specify an override username for HTTP authentication for Cloudera Repositories. You must also specify an HTTP authentication override password.

Related Name

Default Value

API Name

remote_repo_override_user

Required

false

Other

ECS App Domain Unique Regex

Description

The regex used to identify the unique portion of the App domain name that will be extracted and used as the default environment name generated during ECS installation. There can only be one unique portion of the regex and it must be enclosed in parentheses. The default regex will use the first layer of the App Domain name as the default environment name. e.g. With an App Domain name "cloudera-test.cloudera.com", "cloudera-test" will be used as the default environment name.

Related Name

Default Value

^([^.]*)

API Name

app_domain_unique_regex

Required

false

CDP Private Cloud Repository URLs

Description

URLs of the remote repositories where Cloudera Manager can download the CDP Private Cloud installer. There should be a manifest.json under these URLs. If you are using local mirror repositories, do not delete these local mirrors until after the corresponding CDP Private Cloud deployment has been upgraded or uninstalled.

Related Name

Default Value

https://archive.cloudera.com/p/cdp-pvc-ds/latest

API Name

cdppc_repo_urls

Required

false

Custom Banner Text

Description

The custom banner is used to display customer specific text in the header area.

Related Name

Default Value

API Name

custom_banner_html

Required

false

Custom Header Color

Description

The custom header color is used to distinguish different instances of Cloudera Manager.

Related Name

Default Value

BLACK

API Name

custom_header_color

Required

true

Custom Information Assurance Policy Text

Description

An information assurance policy statement that must be agreed to in order for a user to login.

Related Name

Default Value

API Name

custom_ia_policy

Required

false

Delete idle host principals (FreeIPA only)

Description

Delete idle host principals when no service principals are running on the hosts. Only applies when FreeIPA is used as the Kerberos KDC.

Related Name

Default Value

false

API Name

delete_host_principal_ipa

Required

true

Enable Embedded Database Check

Description

When this option is unchecked, warnings about the embedded PostgreSQL database are suppressed.

Related Name

Default Value

true

API Name

enable_embedded_db_check

Required

false

Enable Events Widget Auto-Search

Description

When enabled, the Events widget at the bottom of many pages will auto-fire its default search on page load.

Related Name

Default Value

true

API Name

events_widget_search_on_load

Required

true

Maximum Cluster Count Shown In Full

Description

When the number of clusters exceeds this number, only the cluster summary information will be shown on the home page.

Related Name

Default Value

2

API Name

home_page_full_limit

Required

true

System Identifier

Description

An identifier for this system, to be included with diagnostic data bundles.

Related Name

Default Value

default

API Name

system_identifier

Required

true

Parcels

Automatically Distribute Available Parcels

Description

Whether available parcels should be automatically distributed to any cluster that already has parcels of the same product.

Related Name

Default Value

false

API Name

distribute_parcels_automatically

Required

true

Automatically Download New Parcels

Description

Whether new parcels discovered on the remote parcel repository should be automatically downloaded.

Related Name

Default Value

false

API Name

download_parcels_automatically

Required

true

Cloudera Manager Manages Parcels

Description

Whether Cloudera Manager should manage which parcels should be present on all managed hosts.

Related Name

Default Value

true

API Name

manages_parcels

Required

true

Automatically Downloaded Products

Description

If automatic parcel downloading is enabled, the list of products that will be downloaded.

Related Name

Default Value

CDH

API Name

parcel_autodownload_products

Required

false

Automatically Remove Old Parcels

Description

Whether parcels for old versions of an activated product should be removed from a cluster when they are no longer in use.

Related Name

Default Value

false

API Name

parcel_cleanup_automatically

Required

true

Number of Old Parcel Versions to Retain

Description

If automatic removal of old parcels is enabled, this specifies the number of old parcels to keep. Any old parcels beyond this value will be removed. If this is set to zero, no old parcels will be retained.

Related Name

Default Value

3

API Name

parcel_cleanup_threshold

Required

true

Parcel Distribution Rate Limit

Description

Per-second rate limit for parcel distribution. The default of 50MiB/second allows for parcel distribution to saturate about half of a Gigabit link.

Related Name

Default Value

50 MiB

API Name

parcel_distribute_rate_limit_kbs_per_second

Required

true

Automatically Install CSD Repo URLs

Description

Each CSD may specify a parcel repo URL. If set to true, Cloudera Manager will automatically scan CSDs and add these URLs to the list of parcel repo URLs on every startup of Cloudera Manager. Uncheck this if you only want custom URLs to be present in the list.

Related Name

Default Value

true

API Name

parcel_install_csd_repo_urls

Required

false

Maximum Parcel Uploads

Description

Maximum number of concurrent uploads allowed to distribute parcels to individual hosts. The maximum allowed number of concurrent uploads is 50.

Related Name

Default Value

10

API Name

parcel_max_upload

Required

true

Apply Permissions with respect to files installed by the parcels

Description

Apply Permissions for files installed by the parcels

Related Name

Default Value

true

API Name

parcel_permissions

Required

true

Validate Parcel Relations

Description

Enforce that parcel dependencies are satisfied and conflicts are prevented when activating parcels. Parcel relations (Depends, Conflicts, and Replaces) can be defined in the manifests of parcel repositories. Cloudera Manager can also enforce some default relations if none are defined in the manifest.

Related Name

Default Value

true

API Name

parcel_relation_validation

Required

true

Local Parcel Repository Path

Description

Path to the local package parcel repository from which binaries are served to the Agents.

Related Name

Default Value

/opt/cloudera/parcel-repo

API Name

parcel_repo_path

Required

true

Create System-Wide Symlinks for Active Parcels

Description

Whether system-wide symlinks should be created for the active parcels (for example, /usr/bin/hadoop).

Related Name

Default Value

true

API Name

parcel_symlinks

Required

true

Parcel Update Frequency

Description

How often to check local and remote parcel repositories for new parcels and if any old parcels should be cleaned up. Setting a value of 0 disables the parcel check.

Related Name

Default Value

1 hour(s)

API Name

parcel_update_freq

Required

true

Create Users and Groups for Parcels

Description

Whether a parcel's specified users, groups created. This may not be desired if custom users and groups are being used, or if they have to be created externally.

Related Name

Default Value

true

API Name

parcel_users_groups

Required

true

Remote Parcel Repository URLs

Description

URLs of the remote parcel repositories where Cloudera Manager checks for new parcels. When checking for new parcels, Cloudera Manager sends the ID of the server and the server version to the repository host. The special variable {latest_supported} is replaced with the latest version of CDH that Cloudera Manager supports when checks are made.

Related Name

Default Value

https://archive.cloudera.com/p/cdh7/latest_supported/parcels/ https://archive.cloudera.com/cdh7/latest_supported/parcels/ https://parcels.repos.intel.com/mkl/latest

API Name

remote_parcel_repo_urls

Required

false

Retain Downloaded Parcel Files

Description

Whether downloaded parcel files be kept by Agents after they have been unpacked. Keeping the parcel files consumes additional disk space but allows downloads to be avoided if the parcel ever needs to be unpacked again.

Related Name

Default Value

true

API Name

retain_parcels_in_cache

Required

true

Performance

Send Agent heartbeat every

Description

The interval between each heartbeat that is sent from Agents to the server

Related Name

Default Value

15 second(s)

API Name

heartbeat_interval

Required

true

Agent heartbeat requester

Description

Whether heartbeat request must be made on-demand instead of relying on the next periodic heartbeat. System property setting "cmf.heartbeat.enableExplicit=false" takes precedence over this configuration.

Related Name

Default Value

true

API Name

heartbeat_requester

Required

true

Multithread Configuration Generator Parallelism

Description

Dynamically adjusts how many worker threads will be used to perform configuration generation by the Multithread Configuration Generator. Setting a value of 1 makes the generator work in sequential fashion (zero performance benefit). Higher values allow increased performance. This is recommended to be set to the number of available processor cores (this is the default setting). Adjustments are performed on the fly also when the generator is in operation.

Related Name

Default Value

3

API Name

mt_config_generation_parallelism

Required

false

Ports and Addresses

Agent Port to connect to Server

Description

Specify the port for Agents to use to connect to the Server. Must be 1024 or higher.

Related Name

Default Value

7182

API Name

agent_port

Required

true

Cloudera Manager Hostname Override

Description

Override to use for Cloudera Manager's hostname. Normally this is determined automatically, but this can be used if InetAddress.getLocalhost() is returning the loopback address.

Related Name

Default Value

API Name

cm_host_name

Required

false

Cloudera Manager Frontend URL

Description

If you are using a proxy such as Knox or a load balancer to access Cloudera Manager, specify the frontend URL of that proxy here. This will be used as a prefix for generating URLs and quick links. This should be in the form of https://server:port and should not contain any path information starting at /cmf. After making a change, restart the Event Server role to ensure all emails are generated using this url.

Related Name

frontend_url

Default Value

API Name

frontend_url

Required

false

HTTP Port for Admin Console

Description

Specify the HTTP port to use to access the Server via the Admin Console. Must be 1024 or higher.

Related Name

Default Value

7180

API Name

http_port

Required

true

HTTPS Port for Admin Console

Description

Specify the HTTPS port to use to access the Server via the Admin Console. Must be 1024 or higher.

Related Name

Default Value

7183

API Name

https_port

Required

true

Replication

The Replication page should be always visible

Description

The Replication page is by default not visible for non "Replication Administrator" users. Enable this to allow readonly access to the replication pages for non "Replication Administrator" users.

Related Name

Default Value

false

API Name

bdr_pages_always_visible

Required

true

Custom Kerberos Keytab Location (to be used for replication for secure clusters on this Cloudera Manager)

Description

Define a custom Kerberos keytab location on the Cloudera Manager host to use for replication. If this configuration is specified, the "Custom Kerberos Principal Name" must also be specified. The keytab should be owned by the user running the Cloudera Manager server process (typically "cloudera-scm") and should be configured with a filesystem access control of "0400".

Related Name

Default Value

API Name

bdr_replication_kerberos_keytab_location

Required

false

Custom Kerberos Principal Name (to be used for replication for secure clusters on this Cloudera Manager)

Description

Define a custom Kerberos principal name with an entry in the custom keytab defined in "Custom Kerberos Keytab Location". The principal should be a fully qualified name of an existing principal (eg. adminuser@MY.COMPANY.COM) and the principal must have an entry in the keytab specified in "Custom Kerberos Keytab Location". The principal should also be a superuser in all distributed file system services on secure clusters in this Cloudera Manager.

Related Name

Default Value

API Name

bdr_replication_kerberos_principal_name

Required

false

Reports

Report Configurations

Description

List of configurations for the Cluster Utilization Report.

Related Name

Default Value

[name: Default, tenantType: POOL, daysOfWeek: [], isAllDay: true, startHourOfDay: 0, endHourOfDay: 23 , name: Weekdays, tenantType: POOL, daysOfWeek: [1, 2, 3, 4, 5], isAllDay: true, startHourOfDay: 0, endHourOfDay: 23]

API Name

report_configurations

Required

true

Security

Use TLS Encryption for Agents

Description

Select this option to enable TLS encryption between the Server and Agents.

Related Name

Default Value

false

API Name

agent_tls

Required

false

JKS Keystore File Password for Automatic TLS configuration

Description

The password for JKS keystore file used for automatic TLS configuration of Cloudera Manager server, agent and services.

Related Name

Default Value

API Name

auto_tls_keystore_password

Required

false

JKS Truststore File Password for Automatic TLS configuration

Description

The password for JKS truststore file used for automatic TLS configuration of Cloudera Manager server, agent and services.

Related Name

Default Value

API Name

auto_tls_truststore_password

Required

false

Automatic configuration of TLS for services

Description

Allows automatic configuration of TLS for services using Cloudera Manager's TLS configuration without specifying TLS related settings like keystore path, password etc. for each service.

Related Name

Default Value

NONE

API Name

auto_tls_type

Required

false

Redaction Parameters for Diagnostic Bundles

Description

Note: Do not edit this property in the classic layout. Switch to the new layout to edit and test your rules inline.Use this property to define a list of rules to be followed for redacting sensitive information from diagnostic bundles. Click + to add a new redaction rule. You can choose one of the preconfigured rules or add a custom rule. When specifying a custom rule, the Search field should contain a regular expression to be matched against the data. If a match is found, it is replaced by the contents of the Replace field.Trigger is an optional field. It can be used to specify a simple string to be searched in the data. If the string is found, the redactor attempts to find a match for the Search regex. If no trigger is specified, redaction occurs by matching the Search regular expression. Use the Trigger field to enhance performance: simple string matching is faster than regular expression matching.Test your rules by entering sample text into the Test Redaction Rules text box and clicking Test Redaction. If no rules match, the text you entered is returned unchanged.

Related Name

Default Value

version: 1, rules: [description: Redact passwords from json files, caseSensitive: false, trigger: password, search: \password\[ ]*:[ ]*\[^\]+\, replace: \password\: \BUNDLE-REDACTED \ , description: Redact password= and password:, caseSensitive: false, trigger: password, search: password[:=][^ \\\\\]+, replace: password=BUNDLE-REDACTED , description: Redact passwd= and passwd:, caseSensitive: false, trigger: passwd, search: passwd[:=][^ \\\\\]+, replace: passwd=BUNDLE-REDACTED , description: Redact pass= and pass:, caseSensitive: false, trigger: pass, search: pass[:=][^ \\\\\]+, replace: pass=BUNDLE-REDACTED , description: Redact PASSWORD, , caseSensitive: false, trigger: PASSWORD, , search: PASSWORD, [^\\\\\]+, replace: PASSWORD, BUNDLE-REDACTED , description: Redact key= and key:, caseSensitive: false, trigger: key, search: key[:=][^ \\\\\]+, replace: key=BUNDLE-REDACTED , description: Redact secret= and secret:, caseSensitive: false, trigger: secret, search: secret[:=][^ \\\\\]+, replace: secret=BUNDLE-REDACTED , description: Redact credential= and credential:, caseSensitive: false, trigger: credential, search: credential[:=][^ \\\\\]+, replace: credential=BUNDLE-REDACTED , description: Redact token= and token:, caseSensitive: false, trigger: token, search: token[:=][^ \\\\\]+, replace: token=BUNDLE-REDACTED , description: Redact keyid= and keyid:, caseSensitive: false, trigger: keyid, search: keyid[:=][^ \\\\\]+, replace: keyid=BUNDLE-REDACTED]

API Name

diag_bundle_redaction_policy

Required

false

Host certificate generator command.

Description

Utility to be executed on CM server host to generate certificates for a new host. Host name will be passed as the sole positional argument. The process is expected to write to stdout a zip file containing keys/certificates.

Related Name

Default Value

API Name

host_cert_generator

Required

false

Cloudera Manager TLS/SSL Server Keystore File Password

Description

The password for the Cloudera Manager keystore file.

Related Name

Default Value

API Name

keystore_password

Required

false

Cloudera Manager TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Cloudera Manager is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

Default Value

API Name

keystore_path

Required

false

Java Keystore Type

Description

Type of Java keystore used for all keystores and trust stores. Default value is set to JKS. Some types may require a crypto provider to be configured. Example values: JKS, JCEKS, PKCS12, BCFKS. Note: Default value for CM running in FIPS mode is BCFKS.

Related Name

Default Value

jks

API Name

keystore_type

Required

false

Show Last Login

Description

When enabled, shows the last login details for the current user in the user profile.

Related Name

Default Value

true

API Name

last_login_enabled

Required

false

Verify Agent Hostname Against Certificate

Description

Select this option to verify that agent hostnames must match their TLS client certificates.

Related Name

Default Value

true

API Name

need_agent_hostname_validation

Required

true

Use TLS Authentication of Agents to Server

Description

Select this option to enable TLS Authentication of Agents to the Server.

Related Name

Default Value

false

API Name

need_agent_validation

Required

true

Minimum password length

Description

Minimum number of characters, including letters, digits, and special characters required in the password for local Cloudera Manager users.

Related Name

Default Value

0

API Name

password_min_length

Required

false

Minimum number of digits required in password

Description

Specifies the minimum number of digits required in the password.

Related Name

Default Value

0

API Name

password_min_no_of_digits

Required

false

Minimum number of letters required in password

Description

Specifies the minimum number of letters required in the password.

Related Name

Default Value

0

API Name

password_min_no_of_letters

Required

false

Minimum number of special characters required in password

Description

Specifies the minimum number of non-alphanumeric characters required in the password.

Related Name

Default Value

0

API Name

password_min_no_of_special_chars

Required

false

HTTP Referer Check

Description

Whether to verify "Referer" in HTTP header for state changing requests. This protects against cross-site request forgery, but may need to be turned off if browsers or proxies in your environment do not specify the header.

Related Name

Default Value

true

API Name

referer_check

Required

true

Maximum Number of Active User Sessions

Description

Restrict users to a certain number of active sessions at a time. If set, a user is limited to the specified number of sessions, and the oldest session is terminiated if the user logs in somewhere else. If not set, users can be logged in from as many places as they choose. If the user has 'Remember Me' turned on, or SAML is used for authentication, the user is automatically logged back in each time the session is ended. '0' means no limit is applied.

Related Name

Default Value

0

API Name

session_limit_concurrency

Required

true

Allow 'Remember Me' Option

Description

Whether to allow a user to select 'Remember Me' when logging in. If this is set, the user will not need to log in again for two weeks (unless the server is restarted during that time). If the user chooses 'Remember Me', then the session timeout is ignored.

Related Name

Default Value

true

API Name

session_remember_me

Required

true

Session Timeout

Description

The length of time a user's session can be idle for before the user must log in again.

Related Name

Default Value

30 minute(s)

API Name

session_timeout

Required

true

Show Stacktraces On Error Pages

Description

Control whether stacktraces are shown on error pages. While stacktraces help with debugging, they can sometimes expose sensitive information to a potentially malicious user.

Related Name

Default Value

false

API Name

show_stacktraces

Required

true

Server SSL Certificate Host Name

Description

Host name associated with CM Server SSL certificate to be passed to configuration of newly added host as the host agents are to connect to.

Related Name

Default Value

API Name

ssl_certificate_hostname

Required

false

Supported SSL/TLS versions

Description

The SSL/TLS protocol versions to accept HTTPS connections from. Note that the available cipher suites also affect which protocol versions can be negotiated, and some cipher suites are only available in higher versions.

Related Name

Default Value

TLSv1.2

API Name

supported_tls_versions

Required

true

Cloudera Manager TLS/SSL Trust Store Password

Description

The password for the Cloudera Manager TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

truststore_password

Required

false

Cloudera Manager TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Cloudera Manager might connect to. This trust store must contain the certificate(s) used

to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

truststore_path

Required

false

Use TLS Encryption for Admin Console

Description

Enable TLS encryption (HTTPS) between the user and the Cloudera Manager Admin Console. When checked, the HTTPS port will be used.

Related Name

Default Value

false

API Name

web_tls

Required

false

Support

Audit Records Eviction Frequency

Description

Frequency (in hours) to remove records from Cloudera Manager Audit table. Setting it to 0 will disable this function.

Related Name

Default Value

23 hour(s)

API Name

audit_records_evict_frequency

Required

false

Audit Records batch eviction size

Description

Audit records are removed in batches. This field configures the size of the batch.

Related Name

Default Value

0

API Name

audit_records_evict_no_of_records

Required

false

Audit Records Eviction Control

Description

Enable removal of records from Cloudera Manager Audit table. None means stop removing audit records.

Related Name

Default Value

HOUR

API Name

audit_records_evit_schedule

Required

true

Audit Records Life Time

Description

Remove Audit Records older than the configured date

Related Name

Default Value

API Name

audit_records_life_time

Required

false

Number of Diagnostic Bundles to Keep

Description

The maximum number of command results to keep before deleting them from local storage. This property is used for the commands that generate large result files. A value of -1 indicates no limit.

Related Name

Default Value

10

API Name

cluster_stats_count

Required

false

Scheduled Diagnostic Data Size (MB)

Description

Approximate size in MB of scheduled diagnostic data bundle

Related Name

Default Value

100

API Name

cluster_stats_default_size_mb

Required

false

Use HTTPS to Upload Diagnostic Data

Description

Whether to use HTTPS to upload diagnostic data bundles instead of the now-deprecated SFTP. Uses proxy settings from the network setting.

Related Name

Default Value

true

API Name

cluster_stats_http

Required

true

Diagnostic Data Bundle Directory

Description

Local directory to store diagnostic data bundles. Leave blank to store bundles for 24 hours. This directory must be writable by the cloudera-scm user.

Related Name

Default Value

API Name

cluster_stats_path

Required

false

Scheduled Diagnostic Data Collection Frequency

Description

Frequency of automatically collecting diagnostic data and sending to Cloudera support.

Related Name

Default Value

WEEKLY

API Name

cluster_stats_schedule

Required

true

Scheduled Diagnostic Data Collection Time

Description

Time of day to collect and send diagnostic data to Cloudera

Related Name

Default Value

API Name

cluster_stats_start

Required

false

Diagnostic Data Temp Directory

Description

Local path to assemble diagnostic data bundles. Leave blank to assemble these bundles in your JVM temp directory. Set this value if you run out of disk space while collecting diagnostic data.

Related Name

Default Value

API Name

cluster_stats_tmp_path

Required

false

Collect Cloudera Manager database copy with Diagnostic Data Bundle

Description

Allows the Server to create Cloudera Manager database copy and ship it with diagnostic data bundle for debugging purposes.

Related Name

Default Value

false

API Name

cm_db_dump

Required

true

Cloudera Manager Database Table Names to skip

Description

List of tables to ignore while collecting Cloudera Manager Database dump

Related Name

Default Value

API Name

cm_db_dump_list_to_ignore_tables

Required

false

Cloudera Manager Database bundle size (MB)

Description

The maximum size of the Cloudera Manager database copy to be included with the Diagnostic Bundle

Related Name

Default Value

1024

API Name

cm_db_dump_size_mb

Required

false

Diagnostic Bundle Collection Thread Pool Size

Description

Maximum limit of threads used by Cloudera Manager during diagnostic bundle

Related Name

Default Value

128

API Name

diag_bundle_max_threads

Required

false

Diagnostic Bundle Scale Factor

Description

Scaling factor is directly proportional to the time taken to collect diagnostic bundle. Increase this value to reduce the timeouts during data collection

Related Name

Default Value

0.133

API Name

diag_bundle_scale_out_factor

Required

false

Send Diagnostic Data to Cloudera Automatically

Description

Allows the Server to automatically send diagnostic data when a collection is triggered.

Related Name

Default Value

true

API Name

phone_home

Required

true

Stale Process Threshold Days

Description

Stale processes are ones that have been stopped. Cloudera Manager removes information about these stale processes from the Cloudera Manager Database after a configurable number of days. This field allows changing that number of days.

Related Name

Default Value

1 day(s)

API Name

stale_process_threshold

Required

false

Suppressions

Suppress Parameter Validation: Active Directory Account Prefix

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Account Prefix parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ad_account_prefix

Required

true

Suppress Parameter Validation: Active Directory Suffix

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Suffix parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ad_kdc_domain

Required

true

Suppress Parameter Validation: Active Directory LDAP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory LDAP Port parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ad_ldap_port

Required

true

Suppress Parameter Validation: Active Directory LDAPS Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory LDAPS Port parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ad_ldaps_port

Required

true

Suppress Parameter Validation: Agent Port to connect to Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Agent Port to connect to Server parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_agent_port

Required

true

Suppress Parameter Validation: ECS App Domain Unique Regex

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the ECS App Domain Unique Regex parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_app_domain_unique_regex

Required

true

Suppress Parameter Validation: External Authentication Program Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the External Authentication Program Path parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_auth_script

Required

true

Suppress Parameter Validation: JKS Keystore File Password for Automatic TLS configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JKS Keystore File Password for Automatic TLS configuration parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_auto_tls_keystore_password

Required

true

Suppress Parameter Validation: JKS Truststore File Password for Automatic TLS configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JKS Truststore File Password for Automatic TLS configuration parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_auto_tls_truststore_password

Required

true

Suppress Parameter Validation: Custom Kerberos Keytab Location (to be used for replication for secure clusters on this Cloudera Manager)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Kerberos Keytab Location (to be used for replication for secure clusters on this Cloudera Manager) parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_bdr_replication_kerberos_keytab_location

Required

true

Suppress Parameter Validation: Custom Kerberos Principal Name (to be used for replication for secure clusters on this Cloudera Manager)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Kerberos Principal Name (to be used for replication for secure clusters on this Cloudera Manager) parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_bdr_replication_kerberos_principal_name

Required

true

Suppress Parameter Validation: CDP Private Cloud Repository URLs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the CDP Private Cloud Repository URLs parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cdppc_repo_urls

Required

true

Suppress Parameter Validation: Diagnostic Data Bundle Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Diagnostic Data Bundle Directory parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cluster_stats_path

Required

true

Suppress Parameter Validation: Diagnostic Data Temp Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Diagnostic Data Temp Directory parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cluster_stats_tmp_path

Required

true

Suppress Parameter Validation: Cloudera Manager Database Table Names to skip

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Database Table Names to skip parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cm_db_dump_list_to_ignore_tables

Required

true

Suppress Parameter Validation: Cloudera Manager Hostname Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Hostname Override parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cm_host_name

Required

true

Suppress Parameter Validation: Cloudera Manager Server Local Data Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Server Local Data Storage Directory parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_command_storage_path

Required

true

Suppress Configuration Validator: Multithread Config Generator Parallelism validator

Description

Whether to suppress configuration warnings produced by the Multithread Config Generator Parallelism validator configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_config_gen_executor_parallelism_validator

Required

true

Suppress Parameter Validation: Cross Entity Aggregate Generation Filters

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cross Entity Aggregate Generation Filters parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_cross_entity_aggregate_filters

Required

true

Suppress Parameter Validation: Local Descriptor Repository Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Local Descriptor Repository Path parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_csd_repo_path

Required

true

Suppress Parameter Validation: Custom Banner Text

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Banner Text parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_custom_banner_html

Required

true

Suppress Parameter Validation: Custom Information Assurance Policy Text

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Information Assurance Policy Text parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_custom_ia_policy

Required

true

Suppress Parameter Validation: Redaction Parameters for Diagnostic Bundles

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Redaction Parameters for Diagnostic Bundles parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_diag_bundle_redaction_policy

Required

true

Suppress Parameter Validation: Cloudera Manager Agent Connections Disabled Protocols

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Agent Connections Disabled Protocols parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_disabled_agent_connection_protocols

Required

true

Suppress Parameter Validation: Extra JVM arguments for Java-based services

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Extra JVM arguments for Java-based services parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_extra_jvm_opts

Required

true

Suppress Parameter Validation: Cloudera Manager Frontend URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Frontend URL parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_frontend_url

Required

true

Suppress Parameter Validation: Custom Kerberos Keytab Retrieval Script

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Kerberos Keytab Retrieval Script parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_gen_keytab_script

Required

true

Suppress Parameter Validation: Agent Heartbeat Logging Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Agent Heartbeat Logging Directory parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_heartbeat_logging_dir

Required

true

Suppress Parameter Validation: Host certificate generator command.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host certificate generator command. parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_host_cert_generator

Required

true

Suppress Parameter Validation: HTTP Port for Admin Console

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP Port for Admin Console parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_http_port

Required

true

Suppress Parameter Validation: HTTPS Port for Admin Console

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTPS Port for Admin Console parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_https_port

Required

true

Suppress Parameter Validation: Active Directory Domain Controller Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain Controller Override parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_kdc_account_creation_host_override

Required

true

Suppress Parameter Validation: KDC Admin Server Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the KDC Admin Server Host parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_kdc_admin_host

Required

true

Suppress Parameter Validation: KDC Server Host

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the KDC Server Host parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_kdc_host

Required

true

Suppress Parameter Validation: Cloudera Manager TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_keystore_password

Required

true

Suppress Parameter Validation: Cloudera Manager TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_keystore_path

Required

true

Suppress Parameter Validation: Exclude Users for SPNEGO/Kerberos Authentication

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Exclude Users for SPNEGO/Kerberos Authentication parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_auth_exclude_users

Required

true

Suppress Parameter Validation: Keytab File for SPNEGO Authentication Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Keytab File for SPNEGO Authentication Override parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_auth_keytab

Required

true

Suppress Parameter Validation: Kerberos Principal for SPNEGO Authentication Override

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Principal for SPNEGO Authentication Override parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_auth_principal

Required

true

Suppress Parameter Validation: Domain Name(s)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Domain Name(s) parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_domain

Required

true

Suppress Configuration Validator: Validator for Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf

Description

Whether to suppress configuration warnings produced by the Validator for Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_domain_realm

Required

true

Suppress Parameter Validation: Kerberos Encryption Types

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Encryption Types parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_enc_types

Required

true

Suppress Parameter Validation: KDC Timeout

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the KDC Timeout parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_kdc_timeout

Required

true

Suppress Parameter Validation: krb5.conf file path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the krb5.conf file path parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_krb5_conf_path

Required

true

Suppress Parameter Validation: Advanced Configuration Snippet (Safety Valve) for [libdefaults] section of krb5.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced Configuration Snippet (Safety Valve) for [libdefaults] section of krb5.conf parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_libdefaults_safety_valve

Required

true

Suppress Parameter Validation: Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_other_safety_valve

Required

true

Suppress Parameter Validation: Advanced Configuration Snippet (Safety Valve) for the Default Realm in krb5.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Advanced Configuration Snippet (Safety Valve) for the Default Realm in krb5.conf parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_realms_safety_valve

Required

true

Suppress Parameter Validation: Kerberos Renewable Lifetime

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Renewable Lifetime parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_renew_lifetime

Required

true

Suppress Parameter Validation: Kerberos Ticket Lifetime

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Ticket Lifetime parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_krb_ticket_lifetime

Required

true

Suppress Parameter Validation: LDAP Bind User Distinguished Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind User Distinguished Name parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_bind_dn

Required

true

Suppress Parameter Validation: LDAP Bind Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_bind_pw

Required

true

Suppress Parameter Validation: LDAP Distinguished Name Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Distinguished Name Pattern parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_dn_pattern

Required

true

Suppress Parameter Validation: LDAP Group Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Search Base parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_group_search_base

Required

true

Suppress Parameter Validation: LDAP Group Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Search Filter parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_group_search_filter

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_url

Required

true

Suppress Parameter Validation: LDAP User Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Search Base parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_user_search_base

Required

true

Suppress Parameter Validation: LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Search Filter parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ldap_user_search_filter

Required

true

Suppress Configuration Validator: Mixed Packages And Parcels

Description

Whether to suppress configuration warnings produced by the Mixed Packages And Parcels configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_mixed_packages_and_parcels

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_nt_domain

Required

true

Suppress Parameter Validation: PAM Service Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the PAM Service Name parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_pam_service_name

Required

true

Suppress Parameter Validation: Automatically Downloaded Products

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Automatically Downloaded Products parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_autodownload_products

Required

true

Suppress Parameter Validation: No Proxy List

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the No Proxy List parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_no_proxy_list

Required

true

Suppress Parameter Validation: Proxy Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_proxy_password

Required

true

Suppress Parameter Validation: Proxy Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Port parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_proxy_port

Required

true

Suppress Parameter Validation: Proxy Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Server parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_proxy_server

Required

true

Suppress Parameter Validation: Proxy User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy User parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_proxy_user

Required

true

Suppress Parameter Validation: Local Parcel Repository Path

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Local Parcel Repository Path parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_parcel_repo_path

Required

true

Suppress Parameter Validation: Allowed Groups for Knox Proxy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Groups for Knox Proxy parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_proxyuser_knox_groups

Required

true

Suppress Parameter Validation: Allowed Hosts for Knox Proxy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Hosts for Knox Proxy parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_proxyuser_knox_hosts

Required

true

Suppress Parameter Validation: Knox Proxy Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Knox Proxy Principal parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_proxyuser_knox_principal

Required

true

Suppress Parameter Validation: Allowed Users for Knox Proxy

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Allowed Users for Knox Proxy parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_proxyuser_knox_users

Required

true

Suppress Parameter Validation: Remote Parcel Repository URLs

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Remote Parcel Repository URLs parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_remote_parcel_repo_urls

Required

true

Suppress Parameter Validation: HTTP authentication password override for Cloudera Repositories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP authentication password override for Cloudera Repositories parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_remote_repo_override_password

Required

true

Suppress Parameter Validation: HTTP authentication username override for Cloudera Repositories

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HTTP authentication username override for Cloudera Repositories parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_remote_repo_override_user

Required

true

Suppress Parameter Validation: Report Configurations

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Report Configurations parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_report_configurations

Required

true

Suppress Parameter Validation: SAML Entity Alias

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Entity Alias parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_entity_alias

Required

true

Suppress Parameter Validation: SAML Entity Base URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Entity Base URL parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_entity_base_url

Required

true

Suppress Parameter Validation: SAML Entity ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Entity ID parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_entity_id

Required

true

Suppress Parameter Validation: Alias of SAML Sign/Encrypt Private Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alias of SAML Sign/Encrypt Private Key parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_key_alias

Required

true

Suppress Parameter Validation: SAML Sign/Encrypt Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Sign/Encrypt Private Key Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_key_password

Required

true

Suppress Parameter Validation: SAML Keystore Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Keystore Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_keystore_password

Required

true

Suppress Parameter Validation: Path to SAML Keystore File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML Keystore File parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_keystore_path

Required

true

Suppress Parameter Validation: SAML Login URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Login URL parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_login_url

Required

true

Suppress Parameter Validation: Path to SAML IDP Metadata File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML IDP Metadata File parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_metadata_path

Required

true

Suppress Parameter Validation: SAML Attribute Identifier for User Role

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Attribute Identifier for User Role parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_oid_role

Required

true

Suppress Parameter Validation: SAML Attribute Identifier for User ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Attribute Identifier for User ID parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_oid_user

Required

true

Suppress Parameter Validation: Path to SAML Role Assignment Script

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML Role Assignment Script parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_saml_role_script

Required

true

Suppress Configuration Validator: Cloudera Manager Server Restart

Description

Whether to suppress configuration warnings produced by the Cloudera Manager Server Restart configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_scm_server_restart

Required

true

Suppress Parameter Validation: Kerberos Security Realm

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Security Realm parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_security_realm

Required

true

Suppress Parameter Validation: Server SSL Certificate Host Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Server SSL Certificate Host Name parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_ssl_certificate_hostname

Required

true

Suppress Parameter Validation: System Identifier

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Identifier parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_system_identifier

Required

true

Suppress Configuration Validator: Tags Limit Validator

Description

Whether to suppress configuration warnings produced by the Tags Limit Validator configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_tags_limit

Required

true

Suppress Configuration Validator: TLS With Kerberos Validator

Description

Whether to suppress configuration warnings produced by the TLS With Kerberos Validator configuration validator.

Related Name

Default Value

false

API Name

scm_config_suppression_tls_with_kerberos_validator

Required

true

Suppress Parameter Validation: Kerberos Trusted Realms

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kerberos Trusted Realms parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_trusted_realms

Required

true

Suppress Parameter Validation: Cloudera Manager TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_truststore_password

Required

true

Suppress Parameter Validation: Cloudera Manager TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

scm_config_suppression_truststore_path

Required

true

Cloudera Management Service

Role groups:

Activity Monitor - Unsupported Since 7.0.0

Advanced

Activity Monitor - Unsupported Since 7.0.0 Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

ACTIVITYMONITOR_role_env_safety_valve

Required

false

Event Publication Maximum Queue Size

Description

The maximum size of the queue in which events published from this role will be buffered. If this queue becomes full (for example, due to an outage), subsequent events will be dropped.

Related Name

activityevents.event.publish.queue.max

Default Value

20000

API Name

actmon_event_publication_queue_size_max

Required

true

Event Publication Retry Period

Description

If an event cannot be delivered immediately by this role, this value controls how long to wait before Event Publisher retries delivery.

Related Name

activityevents.event.publish.retry.ms

Default Value

5000

API Name

actmon_event_publication_retry_period

Required

true

Java Configuration Options for Activity Monitor - Unsupported Since 7.0.0

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

firehose_java_opts

Required

false

Activity Monitor - Unsupported Since 7.0.0 Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

For advanced use only. A string to be inserted into cmon.conf for this role only.

Related Name

Default Value

API Name

firehose_safety_valve

Required

false

Activity Monitor - Unsupported Since 7.0.0 Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Database

Activity Monitor - Unsupported Since 7.0.0 Database Hostname

Description

Name of host where Activity Monitor - Unsupported Since 7.0.0's database is running. It is highly recommended that this database is on the same host as the Activity Monitor - Unsupported Since 7.0.0. If the database is not running on its default port, specify the port number using this syntax: 'host:port'

Related Name

Default Value

localhost

API Name

firehose_database_host

Required

false

Activity Monitor - Unsupported Since 7.0.0 Database Name

Description

Name of the Activity Monitor - Unsupported Since 7.0.0's database.

Related Name

Default Value

firehose

API Name

firehose_database_name

Required

true

Activity Monitor - Unsupported Since 7.0.0 Database Password

Description

Password for logging in to the Activity Monitor - Unsupported Since 7.0.0 database

Related Name

db.hibernate.connection.password

Default Value

API Name

firehose_database_password

Required

false

Activity Monitor - Unsupported Since 7.0.0 Database Type

Description

Type of database to use for Activity Monitor - Unsupported Since 7.0.0.

Related Name

Default Value

mysql

API Name

firehose_database_type

Required

false

Activity Monitor - Unsupported Since 7.0.0 Database Username

Description

Username for logging in to the Activity Monitor - Unsupported Since 7.0.0 database.

Related Name

db.hibernate.connection.username

Default Value

firehose

API Name

firehose_database_user

Required

true

Logs

Activity Monitor - Unsupported Since 7.0.0 Logging Threshold

Description

The minimum log level for Activity Monitor - Unsupported Since 7.0.0 logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Activity Monitor - Unsupported Since 7.0.0 Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Activity Monitor - Unsupported Since 7.0.0 logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Activity Monitor - Unsupported Since 7.0.0 Max Log Size

Description

The maximum size, in megabytes, per log file for Activity Monitor - Unsupported Since 7.0.0 logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Activity Monitor - Unsupported Since 7.0.0 Log Directory

Description

Location of log files for Activity Monitor - Unsupported Since 7.0.0

Related Name

Default Value

/var/log/cloudera-scm-firehose

API Name

mgmt_log_dir

Required

false

Monitoring

Activity Monitor Activity Monitor Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Activity Monitor activity monitor pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

activitymonitor_activity_monitor_pipeline_thresholds

Required

false

Activity Monitor Activity Monitor Pipeline Monitoring Time Period

Description

The time period over which the Activity Monitor activity monitor pipeline will be monitored for dropped messages.

Related Name

Default Value

5 minute(s)

API Name

activitymonitor_activity_monitor_pipeline_window

Required

false

Activity Monitor Activity Tree Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Activity Monitor activity tree pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

activitymonitor_activity_tree_pipeline_thresholds

Required

false

Activity Monitor Activity Tree Pipeline Monitoring Time Period

Description

The time period over which the Activity Monitor activity tree pipeline will be monitored for dropped messages.

Related Name

Default Value

5 minute(s)

API Name

activitymonitor_activity_tree_pipeline_window

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

activitymonitor_fd_thresholds

Required

false

Activity Monitor - Unsupported Since 7.0.0 Host Health Test

Description

When computing the overall Activity Monitor - Unsupported Since 7.0.0 health, consider the host's health.

Related Name

Default Value

true

API Name

activitymonitor_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

activitymonitor_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

activitymonitor_pause_duration_window

Required

false

Activity Monitor - Unsupported Since 7.0.0 Process Health Test

Description

Enables the health test that the Activity Monitor - Unsupported Since 7.0.0's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

activitymonitor_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

activitymonitor_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

activitymonitor_web_metric_collection_thresholds

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

scm_descriptor_age_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Event Publication Log Quiet Time Period

Description

To avoid producing excessive amounts of log output, the Event Publisher component of this role is limited to emitting one message per time period. This value controls the size of that time period.

Related Name

activityevents.event.publish.log.suppress.window.ms

Default Value

1 minute(s)

API Name

actmon_event_publication_log_suppress_window

Required

true

Use the Authentication Service to enable Single Sign On

Description

Use the Authentication Service to enable Single Sign On for the Firehose debug servers. Requires a running Authentication Service.

Related Name

debug.servlet.auth.enabled

Default Value

false

API Name

debug_servlet_auth_enabled

Required

false

Purge Activities Data at This Age

Description

In Activity Monitor, purge data about MapReduce jobs and aggregate activities when the data reaches this age in hours. By default, Activity Monitor keeps data about activities for 336 hours (14 days).

Related Name

firehose.activity.purge.duration.hours

Default Value

14 day(s)

API Name

firehose_activity_purge_duration_hours

Required

false

Purge Attempts Data at This Age

Description

In the Activity Monitor, purge data about MapReduce attempts when the data reaches this age in hours. Because attempt data may consume large amounts of database space, you may wish to purge it more frequently than activity data. By default, Activity Monitor keeps data about attempts for 336 hours (14 days).

Related Name

firehose.attempt.purge.duration.hours

Default Value

14 day(s)

API Name

firehose_attempt_purge_duration_hours

Required

false

Starting Interval for Descriptor Fetch Attempts

Description

The starting interval between fetch attempts for the SCM descriptor when Cloudera Management Service roles are starting. The interval is increased by an additional one second with each failed fetch attempt.

Related Name

mgmt.descriptor.fetch.frequency

Default Value

2 second(s)

API Name

mgmt_descriptor_fetch_frequency

Required

true

Descriptor Fetch Max Attempts

Description

Maximum number of attempts to fetch the SCM descriptor when Cloudera Management Service roles are starting. If the roles are not able to get the descriptor in this number of attempts, then the roles exit.

Related Name

mgmt.num.descriptor.fetch.tries

Default Value

10

API Name

mgmt_num_descriptor_fetch_tries

Required

true

Purge MapReduce Service Data at This Age

Description

The number of hours of past service-level data to keep in the Activity Monitor database, such as total slots running. The default is to keep data for 336 hours (14 days).

Related Name

timeseries.expiration.hours

Default Value

14 day(s)

API Name

timeseries_expiration_hours

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Bind Activity Monitor - Unsupported Since 7.0.0 to Wildcard Address

Description

If enabled, the Activity Monitor - Unsupported Since 7.0.0 binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

amon_bind_wildcard

Required

false

Activity Monitor - Unsupported Since 7.0.0 Web UI Port

Description

Port for Activity Monitor - Unsupported Since 7.0.0's Debug page. Set to -1 to disable the debug server.

Related Name

debug.servlet.port

Default Value

8087

API Name

firehose_debug_port

Required

false

Activity Monitor - Unsupported Since 7.0.0 Listen Port

Description

Port where Activity Monitor - Unsupported Since 7.0.0 is listening for agent messages.

Related Name

firehose.server.port

Default Value

9999

API Name

firehose_listen_port

Required

false

Activity Monitor - Unsupported Since 7.0.0 Nozzle Port

Description

Port where Activity Monitor - Unsupported Since 7.0.0's query API is exposed.

Related Name

nozzle.server.port

Default Value

9998

API Name

firehose_nozzle_port

Required

false

Resource Management

Java Heap Size of Activity Monitor - Unsupported Since 7.0.0 in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

firehose_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Activity Monitor Kerberos Principal

Description

Kerberos principal used by the Activity Monitor. Note: Activity Monitoring should always use the principal used by Hue service.

Related Name

Default Value

hue

API Name

kerberos_role_princ_name

Required

true

Enable TLS/SSL for Firehose Debug Server

Description

Encrypt communication between clients and Firehose Debug Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

debug.servlet.https.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Firehose Debug Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

debug.servlet.https.keystorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Password

Description

The password for the Firehose Debug Server keystore file.

Related Name

debug.servlet.https.keystorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_activitymonitor_role_env_safety_valve

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Database Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_host

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_name

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_password

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Database Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_user

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_debug_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Activity Monitor - Unsupported Since 7.0.0

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Activity Monitor - Unsupported Since 7.0.0 parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_java_opts

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Listen Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Listen Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_listen_port

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Nozzle Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Nozzle Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_nozzle_port

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Advanced Configuration Snippet (Safety Valve) for cmon.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Activity Monitor Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Activity Monitor - Unsupported Since 7.0.0 Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Activity Monitor - Unsupported Since 7.0.0 Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Activity Monitor Pipeline

Description

Whether to suppress the results of the Activity Monitor Pipeline heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_activity_monitor_pipeline

Required

true

Suppress Health Test: Activity Tree Pipeline

Description

Whether to suppress the results of the Activity Tree Pipeline heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_activity_tree_pipeline

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_pause_duration

Required

true

Suppress Health Test: Cloudera Manager Descriptor Age

Description

Whether to suppress the results of the Cloudera Manager Descriptor Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_scm_descriptor_fetch

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_activity_monitor_web_metric_collection

Required

true

Alert Publisher

Advanced

Java Configuration Options for Alert Publisher

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

alertpublisher_java_opts

Required

false

Alert Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

ALERTPUBLISHER_role_env_safety_valve

Required

false

Alert Publisher Advanced Configuration Snippet (Safety Valve) for alertpublisher.conf

Description

For advanced use only. A string to be inserted into alertpublisher.conf for this role only.

Related Name

Default Value

API Name

alertpublisher_safety_valve

Required

false

Alert Publisher Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Alert Publisher Logging Threshold

Description

The minimum log level for Alert Publisher logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Alert Publisher Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Alert Publisher logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Alert Publisher Max Log Size

Description

The maximum size, in megabytes, per log file for Alert Publisher logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Alert Publisher Log Directory

Description

Directory where Alert Publisher will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-alertpublisher

API Name

mgmt_log_dir

Required

false

Monitoring

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

alertpublisher_fd_thresholds

Required

false

Alert Publisher Host Health Test

Description

When computing the overall Alert Publisher health, consider the host's health.

Related Name

Default Value

true

API Name

alertpublisher_host_health_enabled

Required

false

Alert Publisher Process Health Test

Description

Enables the health test that the Alert Publisher's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

alertpublisher_scm_health_enabled

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be

promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Alerts: Enable Email Alerts

Description

This setting allows you to turn email alert delivery on and off.

Related Name

mailserver.enabled

Default Value

true

API Name

alert_mailserver_enabled

Required

false

Alert: Mail From Address

Description

The 'From' address to use for alert emails

Related Name

Default Value

noreply@localhost

API Name

alert_mailserver_from_address

Required

false

Alerts: Mail Server Hostname

Description

The IP address or hostname of the mail server to send alerts to

Related Name

Default Value

localhost

API Name

alert_mailserver_hostname

Required

true

Alerts: Mail Server Password

Description

The password to use to log into the mail server. Warning: this password will be sent over the network to the Alert Publisher host in clear text. In addition, the password will be stored in a plain text file on the Alert Publisher host with restrictive file system permissions.

Related Name

Default Value

API Name

alert_mailserver_password

Required

false

Alerts: Mail Server Protocol

Description

The protocol to use for sending email alerts.

Related Name

Default Value

smtp

API Name

alert_mailserver_protocol

Required

true

Alerts: Mail Message Recipients

Description

A comma-separated list of email addresses to send alerts to

Related Name

Default Value

root@localhost

API Name

alert_mailserver_recipients

Required

true

Alerts: Mail Server Username

Description

The username to use to log into the mail server

Related Name

Default Value

API Name

alert_mailserver_username

Required

false

Custom Alert Script

Description

If configured, this script is invoked on the machine hosting the alert publisher role. The script must be readable and executable by the cloudera-scm user. The script is passed, as a single argument, a path to a UTF-8 JSON file containing a list of alerts. Alerts are, by default, batched over time, and the batch size and the batch interval are configurable with the "Alert Publisher: Maximum Batch Size" and "Alert Publisher: Maximum Batch Interval" configuration options. The alerts file is deleted when the script finishes executing. Only one instance of this script is invoked at any given time, and the script must terminate. The standard out and standard error messages from this script are logged to the alert publisher role's log file.

Related Name

alert.script.path

Default Value

API Name

alert_script_path

Required

false

Alert Publisher: Maximum Batch Size

Description

The Alert Publisher can be configured to batch multiple alerts into a single email. This setting specifies the maximum number of alerts that will be batched into a single email (regardless of the batch interval).

Related Name

alert.aggregate.maxSize

Default Value

32

API Name

alertpublisher_aggregate_max_size

Required

false

Alert Publisher: Maximum Batch Interval

Description

The Alert Publisher can be configured to batch multiple alerts into a single email. This setting specifies the maximum amount of time (in milliseconds) that the Alert Publisher waits before sending an email of the current batch.

Related Name

alert.aggregate.timeout.millis

Default Value

1 minute(s)

API Name

alertpublisher_aggregate_timeout

Required

false

Alert rules for email alerting

Description

An alert rule defines which hosts / services / roles / health test alerts should be sent to which email addresses. Any number of alert rules can be created. If the alert matches to an alert rule, the alert rules with the lower priority won't be processed. Each alert rule has all of the following fields:

- severity - One of these values "WARNING" , "CRITICAL", "BOTH". This defines the level of the alert severity.
- priority - Defines the order of the alert rule processing. The alert rule with the lowest priority will be processed first. Must be a non-negative integer.
- userProfiles - Defines which users should get the email alert. Any number of predefined user profiles can be listed there. If there are more than one profile here, the email alert will be sent to more addresses. If the field remains empty that means that the alerts won't be sent to anyone.
- clusters - Clusters that should be included to the alert rule. Can be an empty list.
- hosts - Hosts that should be included to the alert rule in addition to the host groups. Can be an empty list.
- services - Services that should be included to the alert rule in addition to the service groups. Can be an empty list.
- roles - Roles that should be included to the alert rule in addition to the role groups. Can be an empty list.
- hostGroups - Hosts that should be included to the alert rule. Any number of predefined host groups can be listed there. Can be an empty list. See "Host groups for email alerting".
- serviceGroups - Services that should be included to the alert rule. Any number of predefined service groups can be listed there. Can be an empty list. See "Service groups for email alerting".
- serviceTypes - Include all instances of a specific service. Can be an empty list.
- roleGroups - Roles that should be included to the alert rule. Any number of predefined role groups can be listed there. Can be an empty list. See "Role groups for email alerting".
- roleTypes - Include all instances of a specific role. Can be an empty list.
- healthTests - Include specific health tests. Can be an empty list.

Example:{ "alertRules": [{ "severity": "WARNING", "priority": 0, "userProfiles": "Admins", "clusters": "Cluster 1" }]}

Related Name

alertpublisher.alert.rules

Default Value

API Name

alertpublisher_alert_rules

Required

false

Alerts: Email footer

Description

Optional. If not empty, the text entered here will be inserted verbatim as a footer in HTML and plain-text emails.

Related Name

alert.email.footer

Default Value

API Name

alertpublisher_email_footer

Required

false

Alerts: Email header

Description

Optional. If not empty, the text entered here will be inserted verbatim as a header in HTML and plain-text emails.

Related Name

alert.email.header

Default Value

API Name

alertpublisher_email_header

Required

false

Host groups for email alerting

Description

A host group defines a subset of hosts which can be used as one logical unit for email alerting. Any number of host groups can be created. Each host group must have all of the following fields:

- key - Name of the host group, which should be unique.
- value - Comma-separated list of host names. These should be valid host names or you'll get a validation error. In case of an empty list, it'll define a host group with all managed hosts.

Example:{ "keyValues": [{ "key": "ManagementHosts", "value": "management-1.host.company.site,management-2.host.company.site" }]}

Related Name

alertpublisher.host.groups

Default Value

API Name

alertpublisher_host_groups

Required

false

Role groups for email alerting

Description

A role group defines a subset of roles which can be used as one logical unit for email alerting. Any number of role groups can be created. Each role group must have all of the following fields:

- key - Name of the role group, which should be unique.
- value - Comma-separated list of role names. These should be the role names displayed in the Events page's filter or you'll get a validation error. In case of an empty list, it'll define a role group with all managed roles.

Example:{ "keyValues": [{ "key": "Roles", "value": "DataNode (hdfs-1),DataNode (hdfs-2)" }]}

Related Name

alertpublisher.role.groups

Default Value

API Name

alertpublisher_role_groups

Required

false

Service groups for email alerting

Description

A service group defines a subset of services which can be used as one logical unit for email alerting. Any number of service groups can be created. Each service group must have all of the following fields:

- key - Name of the service group, which should be unique.
- value - Comma-separated list of service names. These should be the service names displayed on the service status pages or you'll get a validation error. In case of an empty list, it'll define a service group with all managed services.

Example:{ "keyValues": [{ "key": "StorageServices", "value": "HBASE-1,HDFS-1" }]}

Related Name

alertpublisher.service.groups

Default Value

API Name

alertpublisher_service_groups

Required

false

User profiles for email alerting

Description

A user profile defines a user who should get the email alerts. Any number of user profiles can be created. Each user profile must have all of the following fields:

- key - Name of the user profile, which should be unique.
- value - Comma-separated list of email addresses.

Example:{ "keyValues": [{ "key": "SysAdmins", "value": "sysadmin1@company.com,sysadmin2@company.com" }, { "key": "Admins", "value": "admin1@company.com,admin2@company.com" }]}

Related Name

alertpublisher.user.profiles

Default Value

API Name

alertpublisher_user_profiles

Required

false

Alerts: Mail Message Format

Description

The format of the email alert message. The 'JSON' format is easy for scripts/programs to parse. The 'HTML' and 'text' formats are designed to be easily read by people.

Related Name

mail.format

Default Value

html

API Name

mail_format

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Alerts: Mail Server TCP Port

Description

Optional. The TCP port where the mail server is listening. If not specified, defaults to 25 if SMTP is selected, or 465 if SMTPS is selected.

Related Name

Default Value

API Name

alert_mailserver_port

Required

false

Alerts: Listen Port

Description

Port where the Alert Publisher listens for internal API requests.

Related Name

alertpublisher.internalapi.port

Default Value

10101

API Name

alertpublisher_internalapi_port

Required

false

Resource Management

Java Heap Size of Alert Publisher in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

256 MiB

API Name

alert_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command:

resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not

managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

SNMP

SNMP Authentication Protocol Pass Phrase

Description

Pass phrase to use for SNMP authentication protocol

Related Name

alert.snmp.auth.password

Default Value

API Name

alert_snmp_auth_password

Required

false

SNMP Authentication Protocol

Description

Authentication algorithm to use for authentication

Related Name

alert.snmp.auth.protocol

Default Value

SHA

API Name

alert_snmp_auth_protocol

Required

false

SNMPv2 Community String

Description

Community string to use to identify this service. Generated SNMPv2 traps will use this string for authentication purpose.

Related Name

alert.snmp.community

Default Value

API Name

alert_snmp_community

Required

false

SNMP Retry Count

Description

Number of time to try before trap is timed out. If this value is set to '0' the trap will be sent only once.

Related Name

alert.snmp.retries

Default Value

0

API Name

alert_snmp_retries

Required

true

SNMP Server Engine Id

Description

Engine Id to use for authentication and privacy. Engine Id is normally a hexadecimal number (e.g. 8000173e03a0c095f80c68). Engine Id along with pass phrases are used to generate keys for authentication and privacy protocols.

Related Name

alert.snmp.security.engineid

Default Value

API Name

alert_snmp_security_engineid

Required

false

SNMP Security Level

Description

Level of security to use for SNMP v3 protocol. Currently only 'no authentication' and 'authentication with no privacy' is supported. Select 'SNMPv2' to use 'Community String' based SNMPv2 authentication.

Related Name

alert.snmp.security.level

Default Value

SNMPv2

API Name

alert_snmp_security_level

Required

true

SNMP NMS Hostname

Description

Hostname of the SNMP NMS (network management software). It can be a DNS name or IP address of the host listening for SNMP traps and notifications. For reference, here is Cloudera Manager SNMP Mib .

Related Name

alert.snmp.server.hostname

Default Value

API Name

alert_snmp_server_hostname

Required

false

SNMP Server Port

Description

Port number on which SNMP server is listening.

Related Name

alert.snmp.server.port

Default Value

162

API Name

alert_snmp_server_port

Required

true

SNMP Timeout

Description

Time to wait before an SNMP trap is resent or timed out.

Related Name

alert.snmp.timeout

Default Value

5 second(s)

API Name

alert_snmp_timeout

Required

true

SNMP Security UserName

Description

Name of a user to use for SNMP security.

Related Name

alert.snmp.username

Default Value

API Name

alert_snmp_username

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Alert: Mail From Address

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alert: Mail From Address parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_from_address

Required

true

Suppress Parameter Validation: Alerts: Mail Server Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Mail Server Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_hostname

Required

true

Suppress Parameter Validation: Alerts: Mail Server Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Mail Server Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_password

Required

true

Suppress Parameter Validation: Alerts: Mail Server TCP Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Mail Server TCP Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_port

Required

true

Suppress Parameter Validation: Alerts: Mail Message Recipients

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Mail Message Recipients parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_recipients

Required

true

Suppress Parameter Validation: Alerts: Mail Server Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Mail Server Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_username

Required

true

Suppress Parameter Validation: Custom Alert Script

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Alert Script parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_script_path

Required

true

Suppress Parameter Validation: SNMP Authentication Protocol Pass Phrase

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMP Authentication Protocol Pass Phrase parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_auth_password

Required

true

Suppress Parameter Validation: SNMPv2 Community String

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMPv2 Community String parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_community

Required

true

Suppress Parameter Validation: SNMP Server Engine Id

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMP Server Engine Id parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_security_engineid

Required

true

Suppress Parameter Validation: SNMP NMS Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMP NMS Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_server_hostname

Required

true

Suppress Parameter Validation: SNMP Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMP Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_server_port

Required

true

Suppress Parameter Validation: SNMP Security UserName

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SNMP Security UserName parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_username

Required

true

Suppress Parameter Validation: Alerts: Email footer

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Email footer parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_email_footer

Required

true

Suppress Parameter Validation: Alerts: Email header

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Email header parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_email_header

Required

true

Suppress Parameter Validation: Alerts: Listen Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alerts: Listen Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_internalapi_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Alert Publisher

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Alert Publisher parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_java_opts

Required

true

Suppress Parameter Validation: Alert Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alert Publisher Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_role_env_safety_valve

Required

true

Suppress Parameter Validation: Alert Publisher Advanced Configuration Snippet (Safety Valve) for alertpublisher.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alert Publisher Advanced Configuration Snippet (Safety Valve) for alertpublisher.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_safety_valve

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Alert Publisher Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alert Publisher Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Alert Publisher Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alert Publisher Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: SNMP Validator

Description

Whether to suppress configuration warnings produced by the SNMP Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_snmp_validator

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_alert_publisher_unexpected_exits

Required

true

Event Server

Advanced

Java Configuration Options for Event Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

eventserver_java_opts

Required

false

Maximum Number of Events Returned by Any Query

Description

The maximum number of events that any query can return. Note: A high value can increase the amount of memory required by Event Server, as well as affect query response times.

Related Name

eventcatcher.max.query.events

Default Value

10000

API Name

eventserver_max_query_events

Required

true

Maximum Write Queue Length

Description

The maximum number of events that can be queued for write before further requests are rejected

Related Name

eventcatcher.ingest.pipeline.max

Default Value

10000

API Name

eventserver_max_write_queue_size

Required

true

Number of Core Event Writer Threads

Description

The number of threads that Event Server will use to write events to its store concurrently

Related Name

eventcatcher.num.ingest.threads

Default Value

2

API Name

eventserver_num_pipeline_threads

Required

true

Event Server Query Timeout

Description

The amount of time, in milliseconds, that Cloudera Manager and the Alert Publisher will wait for the Event Server to respond to a query.

Related Name

eventserver.query.timeout

Default Value

60000

API Name

eventserver_query_timeout

Required

false

Event Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

EVENTSERVER_role_env_safety_valve

Required

false

Event Server Advanced Configuration Snippet (Safety Valve) for eventserver.conf

Description

For advanced use only. A string to be inserted into eventserver.conf for this role only.

Related Name

Default Value

API Name

eventserver_safety_valve

Required

false

Event Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Logs

Event Server Logging Threshold

Description

The minimum log level for Event Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Event Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Event Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Event Server Max Log Size

Description

The maximum size, in megabytes, per log file for Event Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Event Server Log Directory

Description

Directory where Event Server will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-eventserver

API Name

mgmt_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Event Store Capacity Monitoring Thresholds

Description

The health test thresholds on the number of events in the event store. Specified as a percentage of the maximum number of events in Event Server store.

Related Name

Default Value

Warning: 115.0 %, Critical: 130.0 %

API Name

eventserver_capacity_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

eventserver_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

eventserver_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

eventserver_gc_duration_window

Required

false

Event Server Host Health Test

Description

When computing the overall Event Server health, consider the host's health.

Related Name

Default Value

true

API Name

eventserver_host_health_enabled

Required

false

Event Server Index Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Event Server Index Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

eventserver_index_directory_free_space_absolute_thresholds

Required

false

Event Server Index Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Event Server Index Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Event Server Index Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

eventserver_index_directory_free_space_percentage_thresholds

Required

false

Event Server Process Health Test

Description

Enables the health test that the Event Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

eventserver_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

eventserver_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

eventserver_web_metric_collection_thresholds

Required

false

Event Server Write Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Event Server write pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

eventserver_write_pipeline_thresholds

Required

false

Event Server Write Pipeline Monitoring Time Period

Description

The time period over which the Event Server write pipeline will be monitored for dropped messages.

Related Name

Default Value

5 minute(s)

API Name

eventserver_write_pipeline_window

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

scm_descriptor_age_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Alert On Transitions Out of Alerting Health

Description

If set, the health events for transitions out of an alertable health level will also be considered an alert. For example, consider an entity that is configured to alert when it has bad health. If that entity's health becomes bad, an alert will be generated. If this setting is enabled, an alert will also be generated when it returns to good health. If this setting is disabled, then no alert will be generated when it returns to good health. Note that an entity must have enable_alerts set to true for health alerts to be generated for it. And make sure to reference the per-entity setting to turn on health alerts.

Related Name

Default Value

false

API Name

eventserver_alert_on_transition_out_of_alerting_health_enabled

Required

false

Health Alert Threshold

Description

Threshold at which a health event will be considered an alert. Note that an entity must have enable_alerts set to true for health alerts to be generated for it. And make sure to reference the per-entity setting to turn on health alerts.

Related Name

Default Value

Bad

API Name

eventserver_health_events_alert_threshold

Required

false

Event Server Index Directory

Description

Location of the Lucene index for Event Server

Related Name

eventcatcher.server.lucenedir

Default Value

/var/lib/cloudera-scm-eventserver

API Name

eventserver_index_dir

Required

false

Maximum Number of Events in the Event Server Store

Description

The maximum size of the Event Server store, in events. Once this size is exceeded, events is deleted started with the oldest first until the size of the store returns below this threshold

Related Name

eventcatcher.event.capacity

Default Value

5000000

API Name

eventserver_max_index_size

Required

true

Starting Interval for Descriptor Fetch Attempts

Description

The starting interval between fetch attempts for the SCM descriptor when Cloudera Management Service roles are starting. The interval is increased by an additional one second with each failed fetch attempt.

Related Name

mgmt.descriptor.fetch.frequency

Default Value

2 second(s)

API Name

mgmt_descriptor_fetch_frequency

Required

true

Descriptor Fetch Max Attempts

Description

Maximum number of attempts to fetch the SCM descriptor when Cloudera Management Service roles are starting. If the roles are not able to get the descriptor in this number of attempts, then the roles exit.

Related Name

mgmt.num.descriptor.fetch.tries

Default Value

10

API Name

mgmt_num_descriptor_fetch_tries

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Event Server Web UI Port

Description

Port for the Event Server's Debug page. Set to -1 to disable debug server.

Related Name

eventcatcher.server.debug.port

Default Value

8084

API Name

eventserver_debug_port

Required

false

Event Query Port

Description

Port on which the Event Server listens for queries for events.

Related Name

eventcatcher.server.httpport

Default Value

7185

API Name

eventserver_http_port

Required

false

Event Publish Port

Description

Port on which the Event Server listens for the publication of events.

Related Name

eventcatcher.server.port

Default Value

7184

API Name

eventserver_listen_port

Required

false

Resource Management

Java Heap Size of EventServer in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

event_server_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Event Server Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_debug_port

Required

true

Suppress Parameter Validation: Event Query Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Query Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_http_port

Required

true

Suppress Parameter Validation: Event Server Index Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Index Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_index_dir

Required

true

Suppress Parameter Validation: Java Configuration Options for Event Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Event Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_java_opts

Required

true

Suppress Parameter Validation: Event Publish Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Publish Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_listen_port

Required

true

Suppress Parameter Validation: Event Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: Event Server Advanced Configuration Snippet (Safety Valve) for eventserver.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Advanced Configuration Snippet (Safety Valve) for eventserver.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Event Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Event Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Event Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_audit_health

Required

true

Suppress Health Test: Event Store Size

Description

Whether to suppress the results of the Event Store Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_event_store_size

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_host_health

Required

true

Suppress Health Test: Event Server Index Directory Free Space

Description

Whether to suppress the results of the Event Server Index Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_index_directory_free_space

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_otelcol_health

Required

true

Suppress Health Test: Cloudera Manager Descriptor Age

Description

Whether to suppress the results of the Cloudera Manager Descriptor Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_scm_descriptor_fetch

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_web_metric_collection

Required

true

Suppress Health Test: Write Pipeline

Description

Whether to suppress the results of the Write Pipeline heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_event_server_write_pipeline

Required

true

Host Monitor

Advanced

Java Configuration Options for Host Monitor

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

firehose_java_opts

Required

false

Host Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

For advanced use only. A string to be inserted into cmon.conf for this role only.

Related Name

Default Value

API Name

firehose_safety_valve

Required

false

Host Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

HOSTMONITOR_role_env_safety_valve

Required

false

Host Monitor Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Event Publication Maximum Queue Size

Description

The maximum size of the queue in which events published from this role will be buffered. If this queue becomes full (for example, due to an outage), subsequent events will be dropped.

Related Name

health.event.publish.queue.max

Default Value

20000

API Name

svcmon_event_publication_queue_size_max

Required

true

Event Publication Retry Period

Description

If an event cannot be delivered immediately by this role, this value controls how long to wait before Event Publisher retries delivery.

Related Name

health.event.publish.retry.ms

Default Value

5000

API Name

svcmon_event_publication_retry_period

Required

true

Logs

Host Monitor Logging Threshold

Description

The minimum log level for Host Monitor logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Host Monitor Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Host Monitor logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Host Monitor Max Log Size

Description

The maximum size, in megabytes, per log file for Host Monitor logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Host Monitor Log Directory

Description

Location of log files for Host Monitor

Related Name

Default Value

/var/log/cloudera-scm-firehose

API Name

mgmt_log_dir

Required

false

Monitoring

Metrics Aggregation Run Duration Thresholds

Description

The health test thresholds for monitoring the metrics aggregation run duration.

Related Name

Default Value

Warning: 10 second(s), Critical: 30 second(s)

API Name

aggregation_run_duration_thresholds

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Host Monitor Storage Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Host Monitor Storage Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

firehose_storage_directory_free_space_absolute_thresholds

Required

false

Host Monitor Storage Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Host Monitor Storage Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Host Monitor Storage Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

firehose_storage_directory_free_space_percentage_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

hostmonitor_fd_thresholds

Required

false

Host Monitor Host Health Test

Description

When computing the overall Host Monitor health, consider the host's health.

Related Name

Default Value

true

API Name

hostmonitor_host_health_enabled

Required

false

Host Monitor Host Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Host Monitor host pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

hostmonitor_host_pipeline_thresholds

Required

false

Host Monitor Host Pipeline Monitoring Time Period

Description

The time period over which the Host Monitor host pipeline will be monitored for dropped messages.

Related Name

Default Value

5 minute(s)

API Name

hostmonitor_host_pipeline_window

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

hostmonitor_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

hostmonitor_pause_duration_window

Required

false

Host Monitor Process Health Test

Description

Enables the health test that the Host Monitor's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

hostmonitor_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

hostmonitor_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

hostmonitor_web_metric_collection_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Cloudera Manager Metric Schema Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager metric schema was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

metric_schema_age_thresholds_name

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings

using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

scm_descriptor_age_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Use the Authentication Service to enable Single Sign On

Description

Use the Authentication Service to enable Single Sign On for the Firehose debug servers. Requires a running Authentication Service.

Related Name

debug.servlet.auth.enabled

Default Value

false

API Name

debug_servlet_auth_enabled

Required

false

Host Monitor Storage Directory

Description

The directory where Host Monitor data is stored. The Host Monitor stores metric time series and health information.

Related Name

firehose.storage.base.directory

Default Value

/var/lib/cloudera-host-monitor

API Name

firehose_storage_dir

Required

true

Time-Series Storage

Description

The approximate amount of disk space dedicated to storing time series and health data. Once the store has reached its maximum size, older data is deleted to make room for newer data. The disk usage is approximate because data is deleted only when the limit is reached.Note that Cloudera Manager stores time-series data at a number of different data granularities, and these granularities have different effective retention periods. Specifically, Cloudera Manager stores metric data as both raw data points and ten-minutely, hourly, six-hourly, daily, and weekly summary data points. Raw data consumes the bulk of the allocated storage space, weekly summaries the least. As such, raw data is retained for the shortest amount of time, while weekly summary points are unlikely to ever be deleted.See the "Storage" tab on the 'Host Monitor' -> 'Charts Library' -> 'Host Monitor Storage' page for more information on how space is consumed within the Host Monitor. This tab also shows information about the amount of data retained and time window covered by each data granularity.

Related Name

firehose_time_series_storage_bytes

Default Value

10 GiB

API Name

firehose_time_series_storage_bytes

Required

false

Health Event Startup Policy

Description

This setting controls whether health events are emitted when this monitoring role is started. If set to "none", then no health events are emitted. If set to "bad" then health events are emitted for subjects with bad or concerning health. If set to "all" then health events are emitted for all subjects for all health values. The default is "bad".

Related Name

health.event.publish.startup.policy

Default Value

bad

API Name

health_event_publish_startup_policy

Required

false

Starting Interval for Descriptor Fetch Attempts

Description

The starting interval between fetch attempts for the SCM descriptor when Cloudera Management Service roles are starting. The interval is increased by an additional one second with each failed fetch attempt.

Related Name

mgmt.descriptor.fetch.frequency

Default Value

2 second(s)

API Name

mgmt_descriptor_fetch_frequency

Required

true

Descriptor Fetch Max Attempts

Description

Maximum number of attempts to fetch the SCM descriptor when Cloudera Management Service roles are starting. If the roles are not able to get the descriptor in this number of attempts, then the roles exit.

Related Name

mgmt.num.descriptor.fetch.tries

Default Value

10

API Name

mgmt_num_descriptor_fetch_tries

Required

true

Event Publication Log Quiet Time Period

Description

To avoid producing excessive amounts of log output, the Event Publisher component of this role is limited to emitting one message per time period. This value controls the size of that time period.

Related Name

health.event.publish.log.suppress.window.ms

Default Value

1 minute(s)

API Name

svcmon_event_publication_log_suppress_window

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Host Monitor Web UI Port

Description

Port for Host Monitor's Debug page. Set to -1 to disable the debug server.

Related Name

debug.servlet.port

Default Value

8091

API Name

firehose_debug_port

Required

false

Host Monitor Listen Port

Description

Port where Host Monitor is listening for agent messages.

Related Name

firehose.server.port

Default Value

9995

API Name

firehose_listen_port

Required

false

Host Monitor Nozzle Port

Description

Port where Host Monitor's query API is exposed.

Related Name

nozzle.server.port

Default Value

9994

API Name

firehose_nozzle_port

Required

false

Bind Host Monitor to Wildcard Address

Description

If enabled, the Host Monitor binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

hmon_bind_wildcard

Required

false

Resource Management

Java Heap Size of Host Monitor in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

firehose_heapsize

Required

false

Maximum Non-Java Memory of Host Monitor

Description

The amount of memory the Host Monitor can use off of the Java heap.

Related Name

firehose_non_java_memory_bytes

Default Value

2 GiB

API Name

firehose_non_java_memory_bytes

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Enable TLS/SSL for Firehose Debug Server

Description

Encrypt communication between clients and Firehose Debug Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

debug.servlet.https.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Firehose Debug Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

debug.servlet.https.keystorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Password

Description

The password for the Firehose Debug Server keystore file.

Related Name

debug.servlet.https.keystorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Host Monitor Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_debug_port

Required

true

Suppress Configuration Validator: Host Monitor Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Host Monitor Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_host_monitor_heap_role_validator

Required

true

Suppress Configuration Validator: Host Monitor Off Heap Memory Size Validator

Description

Whether to suppress configuration warnings produced by the Host Monitor Off Heap Memory Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_host_monitor_non_java_memory_role_validator

Required

true

Suppress Parameter Validation: Java Configuration Options for Host Monitor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Host Monitor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_java_opts

Required

true

Suppress Parameter Validation: Host Monitor Listen Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Listen Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_listen_port

Required

true

Suppress Parameter Validation: Host Monitor Nozzle Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Nozzle Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_nozzle_port

Required

true

Suppress Parameter Validation: Host Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_safety_valve

Required

true

Suppress Parameter Validation: Host Monitor Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_storage_dir

Required

true

Suppress Parameter Validation: Host Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_hostmonitor_role_env_safety_valve

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Host Monitor Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Host Monitor Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Host Monitor Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Metrics Aggregation Run Duration Test

Description

Whether to suppress the results of the Metrics Aggregation Run Duration Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_aggregation_run_duration

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_host_health

Required

true

Suppress Health Test: Host Pipeline

Description

Whether to suppress the results of the Host Pipeline heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_host_pipeline

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_log_directory_free_space

Required

true

Suppress Health Test: Cloudera Manager Metric Schema Age

Description

Whether to suppress the results of the Cloudera Manager Metric Schema Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_metric_schema_fetch

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_pause_duration

Required

true

Suppress Health Test: Cloudera Manager Descriptor Age

Description

Whether to suppress the results of the Cloudera Manager Descriptor Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_scm_descriptor_fetch

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_scm_health

Required

true

Suppress Health Test: Host Monitor Storage Directory Free Space

Description

Whether to suppress the results of the Host Monitor Storage Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_storage_directory_free_space

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_host_monitor_web_metric_collection

Required

true

Navigator Audit Server

Advanced

Navigator Audit Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for db.navigator.properties

Description

For advanced use only. A string to be inserted into db.navigator.properties for this role only.

Related Name

Default Value

API Name

navigator_db_safety_valve

Required

false

Java Configuration Options for Navigator Audit

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

navigator_java_opts

Required

false

Navigator Audit Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

NAVIGATOR_role_env_safety_valve

Required

false

Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

For advanced use only. A string to be inserted into cloudera-navigator.properties for this role only.

Related Name

Default Value

API Name

navigator_server_safety_valve

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

PII Masking Regular Expression

Description

Regular expression that identifies the strings to be masked. Changing this expression does not mask the strings in previous entries. Leave blank to bypass masking. This feature is superseded by cluster-wide redaction of logs and SQL queries, as an HDFS service-wide configuration parameter.

Related Name

navigator.pii.masking.regex

Default Value

(4[0-9]12(?:[0-9]3)?)|(5[1-5][0-9]14)|(3[47][0-9]13)|(3(?:0[0-5]|[68][0-9])[0-9]11)|(6(?:011|5[0-9]2)[0-9]12)|((?:2131|1800|35\d3)\d11)

API Name

pii_masking_regex

Required

false

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Database

Navigator Audit Server Database Hostname

Description

Name of the host where Navigator Audit Server's database is running. It is highly recommended that this database is on the same host as Navigator Audit Server. If the database is not running on its default port, specify the port number using this syntax: 'host:port'

Related Name

navigator.db.host

Default Value

localhost

API Name

navigator_database_host

Required

false

Navigator Audit Server Database Name

Description

The name of the Navigator Audit Server's database.

Related Name

navigator.db.name

Default Value

nav

API Name

navigator_database_name

Required

true

Navigator Audit Server Database Password

Description

The password for Navigator Audit Server's database user account.

Related Name

navigator.db.password

Default Value

API Name

navigator_database_password

Required

false

Navigator Audit Server Database Type

Description

Type of database used for Navigator Audit Server.

Related Name

navigator.db.type

Default Value

mysql

API Name

navigator_database_type

Required

false

Navigator Audit Server Database Username

Description

The username to use to log into Navigator Audit Server's database.

Related Name

navigator.db.user

Default Value

nav

API Name

navigator_database_user

Required

true

Logs

Navigator Audit Server Logging Threshold

Description

The minimum log level for Navigator Audit Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Navigator Audit Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Navigator Audit Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Navigator Audit Server Max Log Size

Description

The maximum size, in megabytes, per log file for Navigator Audit Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Navigator Audit Server Log Directory

Description

Directory where Navigator Audit Server will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-navigator

API Name

mgmt_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute

- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

navigator_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

navigator_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

navigator_gc_duration_window

Required

false

Navigator Audit Server Host Health Test

Description

When computing the overall Navigator Audit Server health, consider the host's health.

Related Name

Default Value

true

API Name

navigator_host_health_enabled

Required

false

Navigator Audit Server Process Health Test

Description

Enables the health test that the Navigator Audit Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

navigator_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

navigator_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

navigator_web_metric_collection_thresholds

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters,

$ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Navigator Audit Server Data Expiration Period

Description

The number of hours of past audit events to keep in the Navigator Audit Server database. This will affect the size of the database.

Related Name

navigator.db.hours.retained

Default Value

90 day(s)

API Name

hours_retained

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Navigator Audit Server Web UI Port

Description

The port where Navigator Audit Server starts a debug web server. Set to -1 to disable debug server.

Related Name

navigator.server.debug.port

Default Value

8089

API Name

navigator_debug_port

Required

false

Navigator Audit Server Port

Description

The port where Navigator Audit Server listens for requests

Related Name

navigator.server.port

Default Value

7186

API Name

navigator_server_port

Required

false

Publishing

Kafka Topic

Description

The name of the Kafka topic where Navigator will publish audit events.

Related Name

Default Value

NavigatorAuditEvents

API Name

navigator_kafka_publishing_topic

Required

false

Resource Management

Java Heap Size of Auditing Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

navigator_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Navigator Kerberos Principal

Description

Kerberos principal used by Navigator to authenticate to all services except HDFS. Note: Navigator should use the principal used by Hue service if you are using MapReduce1 service in any cluster.

Related Name

Default Value

hue

API Name

kerberos_role_princ_name

Required

true

Navigator TLS/SSL Trust Store File

Description

The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Navigator might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.

Related Name

Default Value

API Name

navigator_truststore_file

Required

false

Navigator TLS/SSL Trust Store Password

Description

The password for the Navigator TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

Default Value

API Name

navigator_truststore_password

Required

false

Enable TLS/SSL for NAVIGATOR

Description

Encrypt communication between clients and NAVIGATOR using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

nav.http.enable_ssl

Default Value

false

API Name

ssl_enabled

Required

false

TLS/SSL Keystore Key Password

Description

The password that protects the private key contained in the keystore used when NAVIGATOR is acting as a TLS/SSL server.

Related Name

nav.ssl.keyManagerPassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

TLS/SSL Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when NAVIGATOR is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

nav.ssl.keyStorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

TLS/SSL Keystore File Password

Description

The password for the NAVIGATOR keystore file.

Related Name

nav.ssl.keyStorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Navigator Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Navigator Audit Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Navigator Audit Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Navigator Audit Server Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Database Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_host

Required

true

Suppress Parameter Validation: Navigator Audit Server Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_name

Required

true

Suppress Parameter Validation: Navigator Audit Server Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_password

Required

true

Suppress Parameter Validation: Navigator Audit Server Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Database Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_user

Required

true

Suppress Parameter Validation: Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for db.navigator.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for db.navigator.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_db_safety_valve

Required

true

Suppress Parameter Validation: Navigator Audit Server Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_debug_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Navigator Audit

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Navigator Audit parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_java_opts

Required

true

Suppress Parameter Validation: Kafka Topic

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Kafka Topic parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_kafka_publishing_topic

Required

true

Suppress Parameter Validation: Navigator Audit Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_role_env_safety_valve

Required

true

Suppress Parameter Validation: Navigator Audit Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_server_port

Required

true

Suppress Parameter Validation: Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_server_safety_valve

Required

true

Suppress Parameter Validation: Navigator TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator TLS/SSL Trust Store File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_truststore_file

Required

true

Suppress Parameter Validation: Navigator TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_truststore_password

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: PII Masking Regular Expression

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the PII Masking Regular Expression parameter.

Related Name

Default Value

false

API Name

role_config_suppression_pii_masking_regex

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: TLS/SSL Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: TLS/SSL Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: TLS/SSL Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigator_web_metric_collection

Required

true

Navigator Metadata Server

Advanced

Allow Usage Data Collection

Description

Allows Cloudera to collect usage data, including the use of Google Analytics.

Related Name

nav.allow_usage_data

Default Value

true

API Name

allow_usage_data

Required

true

Navigator Metadata Server Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Navigator Metadata Server Install Dir

Description

The directory where Navigator Metadata Server is installed. This allows overriding the version packaged with the Cloudera Manager Server.

Related Name

Default Value

API Name

nav_install_dir

Required

false

Navigator Metadata Server Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

For advanced use only, a string to be inserted into the client configuration for navigator.client.properties.

Related Name

Default Value

API Name

navigator_client_config_safety_valve

Required

false

Java Configuration Options for Navigator Metadata Server

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

navigator_java_opts

Required

false

Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

For advanced use only. A string to be inserted into cloudera-navigator.properties for this role only.

Related Name

Default Value

API Name

navigator_safety_valve

Required

false

Navigator Metadata Server Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

NAVIGATORMETASERVER_role_env_safety_valve

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Cloudera Navigator

Enable Audit Collection

Description

Enable collection of audit events from the service's roles.

Related Name

navigator.audit.enabled

Default Value

true

API Name

navigator_audit_enabled

Required

false

Audit Event Filter

Description

Event filters are defined in a JSON object like the following: { "defaultAction" : ("accept", "discard"), "rules" : [{ "action" : ("accept", "discard"), "fields" : [{ "name" : "fieldName", "match" : "regex" }] }] } A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event. A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken. If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object. The following is the list of fields that can be filtered for NAVMS events:

- operation: Navigator operation performed e.g. auditReport, savedSearch etc.
- username: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.

Related Name

navigator.event.filter

Default Value

API Name

navigator_audit_event_filter

Required

false

Database

Navigator Metadata Server Database Hostname

Description

Name of the host where the Navigator Metaserver database is running. If the database is not running on its default port, specify the port number using this syntax: 'host:port'.

Related Name

navms.db.host

Default Value

localhost

API Name

nav_metaserver_database_host

Required

false

Navigator Metadata Server Database Name

Description

The name of the Navigator Metadata Server database.

Related Name

navms.db.name

Default Value

navms

API Name

nav_metaserver_database_name

Required

true

Navigator Metadata Server Database Password

Description

The password for Navigator Metadata Server database user account.

Related Name

navms.db.password

Default Value

API Name

nav_metaserver_database_password

Required

false

Navigator Metadata Server Database Type

Description

Type of database used for Navigator Metadata Server.

Related Name

navms.db.type

Default Value

mysql

API Name

nav_metaserver_database_type

Required

false

Navigator Metadata Server Database Username

Description

The username to use to log into the Navigator Metadata Server database.

Related Name

navms.db.user

Default Value

navms

API Name

nav_metaserver_database_user

Required

true

External Authentication

Authentication Backend Order

Description

The order in which authentication backends are used for authenticating a user. For Cloudera Manager authentication, only users with role 'Full Administrator' and 'Navigator Administrator' are allowed. In addition, users authenticated by Cloudera Manager using external authentication mechanism are not allowed. Navigator will authenticate external users itself and will not rely on Cloudera Manager.

Related Name

nav.auth.backend.order

Default Value

CM_ONLY

API Name

auth_backend_order

Required

true

External Authentication Type

Description

The type of external authentication system to use.

Related Name

nav.external.auth.type

Default Value

LDAP

API Name

external_auth_type

Required

true

Cloudera Navigator S3 Lineage AWS Credentials

Description

Enable Cloudera Navigator to extract metadata and lineage for data that is written to S3 buckets in this account.

Related Name

Default Value

API Name

nav_extraction_external_account

Required

false

LDAP Bind User Distinguished Name

Description

Distinguished name of the user to bind to AD as for user authentication search/bind and group lookup for role authorization. For openLDAP based directories this should be a DN string, for Active Directory this can be just a username, combined with the "Active Directory Domain" value for login. For example username in the field and example.com in the active directory domain will result in the User Principal Name value of username@example.com being used to bind. If you put a UPM value here, do not over-configure the "active directory domain" field otherwise you will end up presenting username@example.com@example.com for binds. AD will accept a UPN value or the DN value as a valid Bind DN; An example of a Distinguished Name (DN): CN=cdh admin,OU=svcaccount,DC=example,DC=com An example of a UPN value: cdhadmin@example.com

Related Name

nav.ldap.bind.dn

Default Value

API Name

nav_ldap_bind_dn

Required

false

LDAP Bind Password

Description

The password of the bind user.

Related Name

nav.ldap.bind.pw

Default Value

API Name

nav_ldap_bind_pw

Required

false

LDAP Distinguished Name Pattern

Description

This setting is deprecated and soon to be removed, do not use LDAP Distinguished Name Pattern for configuration moving forward. It is not necessary to use and deprecated as a configuration approach for LDAP and AD in general.

Related Name

nav.ldap.dn.pattern

Default Value

API Name

nav_ldap_dn_pattern

Required

false

LDAP Group Search Base

Description

The distinguished name indicating the path within the directory information tree to begin group searches from. For example in AD it would be cn=groups,dc=example,dc=com. Or in an openLDAP compatible situation it would be something like ou=groups,dc=example,dc=com. Check with your directory administration team on the proper search base to configure for your environment.

Related Name

nav.ldap.group.search.base

Default Value

API Name

nav_ldap_group_search_base

Required

false

LDAP Group Search Filter For Logged In User

Description

A search filter for finding groups that the logged-in user belongs to. Typically, this is (member={0}), where {0} is replaced by the DN of a successfully authenticated user.

Related Name

nav.ldap.group.search.filter

Default Value

API Name

nav_ldap_group_search_filter

Required

false

LDAP Groups Search Filter

Description

The search filter to use for finding groups for authorization of authenticated users for their cloudera manager role. For Active Directory and openLDAP compatible directories this will usually be (member={0}), where {0} will be replaced by DN string for a successfully authenticated user

through the search/bind process. This requires configuration of the LDAP Bind User Distinguished Name field.

Related Name

nav.ldap.groups.search.filter

Default Value

(&(objectClass=groupOfNames)(cn=*0*))

API Name

nav_ldap_groups_search_filter

Required

false

LDAP URL

Description

The URL of the LDAP Server. The URL must be prefixed with ldap:// or ldaps:// . The URL can optionally specify a custom port if necessary, but by default the ldap:// will connect to port 389, and the ldaps:// will connect to port 636. Note that passwords will be in the clear if ldap:// is used, and by fall 2020 Active directory servers will no longer allow non LDAPS connections to bind to AD hosts with LDAP signing enabled. See microsoft knowledge document 935834 for more information.

Related Name

nav.ldap.url

Default Value

API Name

nav_ldap_url

Required

false

LDAP User Search Base

Description

The distinguished name indicating the path within the directory information tree to begin user searches from. For example in AD it would be cn=users,dc=example,dc=com. Or in an openLDAP compatible situation it would be something like ou=people,dc=example,dc=com. Check with your directory administration team on the proper user search base to configure for your environment.

Related Name

nav.ldap.user.search.base

Default Value

API Name

nav_ldap_user_search_base

Required

false

LDAP User Search Filter

Description

The search filter to use for finding users. For AD configuration it will be (sAMAccountName={0}) and for openLDAP compatible directories it will usually be (uid={0}). Note that a custom attribute can also be used if the directory is configured differently for user names. The {0} expands the currently authenticating user"s name entered in the login form for the query.

Related Name

nav.ldap.user.search.filter

Default Value

API Name

nav_ldap_user_search_filter

Required

false

Active Directory Domain

Description

Use this field for Active Directory configurations only, when combined with a simple username value in the "LDAP Bind User Distinguished Name" field, it will result in a UPM of user@example.com used for search/bind operations for authenticated user lookups.

Related Name

nav.nt_domain

Default Value

API Name

nav_nt_domain

Required

false

SAML Entity Base URL

Description

The Base URL used to construct redirect URLs reported in this server's SP metadata. Leave this blank to let the server calculate the base URL.

Related Name

nav.saml.entity.base_url

Default Value

API Name

nav_saml_entity_base_url

Required

false

SAML Entity ID

Description

The ID that Navigator Metadata Server uses to identify itself to the IDP. This value should be unique to this Navigator Metadata Server installation.

Related Name

nav.saml.entity.id

Default Value

clouderaNavigator

API Name

nav_saml_entity_id

Required

true

Alias of SAML Sign/Encrypt Private Key

Description

The alias used to identify the sign/encrypt private key in the SAML keystore.

Related Name

nav.saml.key.alias

Default Value

API Name

nav_saml_key_alias

Required

false

SAML Sign/Encrypt Private Key Password

Description

The password for the sign/encrypt private key in the SAML keystore.

Related Name

nav.saml.key.password

Default Value

API Name

nav_saml_key_password

Required

false

SAML Keystore Password

Description

The password for the SAML keystore.

Related Name

nav.saml.keystore.password

Default Value

API Name

nav_saml_keystore_password

Required

false

Path to SAML Keystore File

Description

The filesystem path to the keystore file containing the SP private key and any necessary public certificates to validate the IDP.

Related Name

nav.saml.keystore.path

Default Value

API Name

nav_saml_keystore_path

Required

false

SAML Login URL

Description

If your IDP does not support SP-initiated SSO (very uncommon), you use a separate login URL, outside of Navigator Metadata Server. Provide that URL here so that Navigator Metadata Server can use it when a user needs to log in.

Related Name

nav.saml.login.url

Default Value

API Name

nav_saml_login_url

Required

false

Path to SAML IDP Metadata File

Description

The filesystem path to the IDP metadata XML file.

Related Name

nav.saml.metadata.path

Default Value

API Name

nav_saml_metadata_path

Required

false

SAML Attribute Identifier for User Role

Description

The URN OID that identifies the user role in the SAML attributes. Only has an effect when 'Attribute'-based role assignment is used.

Related Name

nav.saml.oid.role

Default Value

urn:oid:2.5.4.11

API Name

nav_saml_oid_role

Required

true

SAML Attribute Identifier for User ID

Description

The URN OID that identifies the user ID in the SAML attributes.

Related Name

nav.saml.oid.user

Default Value

urn:oid:0.9.2342.19200300.100.1.1

API Name

nav_saml_oid_user

Required

true

SAML Response Binding

Description

The SAML binding format that the IDP is asked to use when sending authentication responses.

Related Name

nav.saml.response.binding

Default Value

ARTIFACT

API Name

nav_saml_response_binding

Required

true

SAML Attribute Values for Roles

Description

The values that appear in the SAML role attribute for each Navigator Metadata Server role. The first value corresponds to the Full Administrator role. The second value corresponds to the User Administrator role. The third value corresponds to the Auditing Viewer role. The fourth value corresponds to the Lineage Viewer role. The fifth value corresponds to the Metadata Administrator role. The sixth value corresponds to the Policy Viewer role. The seventh value corresponds to the Policy Administartor role. To assign more than one role, the attribute can return values separated by a comma, like "role1, role2".

Related Name

nav.saml.role.map

Default Value

admin useradmin auditingviewer lineageviewer metadataadmin policyviewer policyadmin

API Name

nav_saml_role_map

Required

true

SAML Role Assignment Mechanism

Description

The mechanism to use for assigning roles to users. 'Attribute' assigns roles based on a SAML attribute. 'Script' assigns roles based on the result of an external script.

Related Name

nav.saml.role.mapper

Default Value

ATTRIBUTE

API Name

nav_saml_role_mapper

Required

true

Path to SAML Role Assignment Script

Description

An external script (or binary) to use to assign roles to SAML users. The username is passed as the first command-line argument. You can configure the return codes for the external script on the Roles page. A negative return value indicates a failure.

Related Name

nav.saml.role.script

Default Value

API Name

nav_saml_role_script

Required

false

Source of User ID in SAML Response

Description

Whether the user ID should be obtained from the SAML response NameID field or from an attribute

Related Name

nav.saml.user.source

Default Value

ATTRIBUTE

API Name

nav_saml_user_source

Required

true

Cloudera Telemetry Publisher S3 Bucket

Description

The name of the S3 bucket where Cloudera Telemetry Publisher from remote clusters will upload metadata to for Cloudera Navigator.

Related Name

nav_telemetry_bucket_name

Default Value

API Name

nav_telemetry_bucket_name

Required

false

Cloudera Telemetry Publisher AWS Credentials

Description

Enable Cloudera Navigator to extract metadata and lineage from other clusters (e.g., Cloudera Altus) collected via Cloudera Telemetry Publisher.

Related Name

Default Value

API Name

nav_telemetry_external_account

Required

false

Extractor Filter

HDFS Filter Enable

Description

Enable HDFS Filtering. When Enabled, filters out the extraction of the items in the blacklist

Related Name

nav.filter.hdfs.enable

Default Value

false

API Name

nav_filter_hdfs_enable

Required

false

HDFS Filter Blacklist

Description

List of paths to be filtered out. The paths can be regular expressions.

Related Name

nav.filter.hdfs.blacklist

Default Value

API Name

nav_filter_hdfs_rules

Required

false

S3 Filter Default Action

Description

Set to Accept to extract all S3 buckets except for the ones blacklisted. Set to Discard to extract only the buckets that are whitelisted.

Related Name

nav.filter.s3.default.action

Default Value

ACCEPT

API Name

nav_filter_s3_default_action

Required

false

S3 Filter Enable

Description

Enable S3 Filtering

Related Name

nav.filter.s3.enable

Default Value

false

API Name

nav_filter_s3_enable

Required

false

S3 Filter list

Description

List of S3 buckets to be whitelisted or blacklisted. The strings can be regular extressions.

Related Name

nav.filter.s3.list

Default Value

API Name

nav_filter_s3_rules

Required

false

Logs

Audit Log Directory

Description

Path to the directory where audit logs will be written. The directory will be created if it doesn't exist.

Related Name

audit_event_log_dir

Default Value

/var/log/cloudera-scm-navigator/audit

API Name

audit_event_log_dir

Required

false

Navigator Metadata Server Logging Threshold

Description

The minimum log level for Navigator Metadata Server logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Navigator Metadata Server Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Navigator Metadata Server logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Navigator Metadata Server Max Log Size

Description

The maximum size, in megabytes, per log file for Navigator Metadata Server logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Navigator Metadata Server Log Directory

Description

Directory where Navigator Metadata Server will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-navigator

API Name

mgmt_log_dir

Required

false

Maximum Audit Log File Size

Description

Maximum size of audit log file in MB before it is rolled over.

Related Name

navigator.audit_log_max_file_size

Default Value

100 MiB

API Name

navigator_audit_log_max_file_size

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Navigator Audit Failure Thresholds

Description

The health test thresholds for failures encountered when monitoring audits within a recent period specified by the mgmt_navigator_failure_window configuration for the role. The value that can be specified for this threshold is the number of bytes of audits data that is left to be sent to audit server.

Related Name

mgmt.navigator.failure.thresholds

Default Value

Warning: Never, Critical: Any

API Name

mgmt_navigator_failure_thresholds

Required

false

Monitoring Period For Audit Failures

Description

The period to review when checking if audits are blocked and not getting processed.

Related Name

mgmt.navigator.failure.window

Default Value

20 minute(s)

API Name

mgmt_navigator_failure_window

Required

false

Navigator Audit Pipeline Health Check

Description

Enable test of audit events processing pipeline. This will test if audit events are not getting processed by Audit Server for a role that generates audit.

Related Name

mgmt.navigator.status.check.enabled

Default Value

true

API Name

mgmt_navigator_status_check_enabled

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

Audit Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Audit Log Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

navigatormetaserver_audit_event_log_directory_free_space_absolute_thresholds

Required

false

Audit Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Audit Log Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Audit Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

navigatormetaserver_audit_event_log_directory_free_space_percentage_thresholds

Required

false

Navigator Metadata Server Storage Dir Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Navigator Metadata Server Storage Dir.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

navigatormetaserver_data_directory_free_space_absolute_thresholds

Required

false

Navigator Metadata Server Storage Dir Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Navigator Metadata Server Storage Dir. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Navigator Metadata Server Storage Dir Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

navigatormetaserver_data_directory_free_space_percentage_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

navigatormetaserver_fd_thresholds

Required

false

Navigator Metadata Server Host Health Test

Description

When computing the overall Navigator Metadata Server health, consider the host's health.

Related Name

Default Value

true

API Name

navigatormetaserver_host_health_enabled

Required

false

Navigator Metadata Server Process Health Test

Description

Enables the health test that the Navigator Metadata Server's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

navigatormetaserver_scm_health_enabled

Required

false

Solr Element Count Threshold

Description

Threshold for throwing alert when the Solr Element Count reaches

Related Name

Default Value

Warning: 5.0E8, Critical: 1.0E9

API Name

navigatormetaserver_solr_element_count_threshold

Required

false

Solr Relation Count Threshold

Description

Threshold for throwing alert when the Solr Relation Count reaches

Related Name

Default Value

Warning: 5.0E8, Critical: 1.0E9

API Name

navigatormetaserver_solr_relation_count_threshold

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Navigator Metadata Server Storage Dir

Description

The directory where Navigator Metadata Server data is stored. Note that changing this location does not migrate existing data.

Related Name

nav.data.dir

Default Value

/var/lib/cloudera-scm-navigator

API Name

data_dir

Required

false

Default Facets

Description

List of metadata properties used by default for Navigator search facets. If no facets are listed, the facets used are some system properties such as "sourceType", "type", "owner", "clusterTemplate", "tags", “deleted”. Your entries here replace these system facets. For example, to include some of the system properties and a managed property "region" in the "sales" namespace, include entries such as "type", "owner", and "sales.region".

Related Name

nav.search.default_facets

Default Value

API Name

nav_search_default_facets

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Policies

Enable Expression Input

Description

Allows policy properties to be specified using Java expressions.

Related Name

nav.policy.expression.enable

Default Value

false

API Name

nav_policies_expression_input

Required

false

JMS Password

Description

The password of the JMS user to which notifications of changes to entities affected by policies are sent.

Related Name

navms.jms.password

Default Value

******

API Name

nav_policies_jms_password

Required

false

JMS Queue

Description

The JMS queue to which notifications of changes to entities affected by policies are sent.

Related Name

navms.jms.queue

Default Value

Navigator

API Name

nav_policies_jms_queue

Required

false

JMS URL

Description

The URL of the JMS server to which notifications of changes to entities affected by policies are sent.

Related Name

navms.jms.url

Default Value

tcp://localhost:61616

API Name

nav_policies_jms_url

Required

false

JMS User

Description

The JMS user to which notifications of changes to entities affected by policies are sent.

Related Name

navms.jms.user

Default Value

admin

API Name

nav_policies_jms_user

Required

false

Ports and Addresses

Navigator Metadata Server Port

Description

The port where Navigator Metadata Server listens for requests

Related Name

nav.http.port

Default Value

7187

API Name

navigator_server_port

Required

false

Resource Management

Java Heap Size of Navigator Metadata Server in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

2 GiB

API Name

navigator_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Navigator Kerberos Principal

Description

Kerberos principal used by Navigator to authenticate to all services except HDFS. Note: Navigator should use the principal used by Hue service if you are using MapReduce1 service in any of the clusters.

Related Name

Default Value

hue

API Name

kerberos_role_princ_name

Required

true

Navigator Kerberos Principal for HDFS

Description

Kerberos principal used by Navigator to authenticate to HDFS services. Note: This principal must have administrator and superuser privileges on all HDFS services.

Related Name

Default Value

hdfs

API Name

nav_hdfs_kerberos_princ

Required

true

Enable TLS/SSL for Navigator Metadata Server

Description

Encrypt communication between clients and Navigator Metadata Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

nav.http.enable_ssl

Default Value

false

API Name

ssl_enabled

Required

false

TLS/SSL Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Navigator Metadata Server is acting as a TLS/SSL server.

Related Name

nav.ssl.keyManagerPassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

TLS/SSL Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Navigator Metadata Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

nav.ssl.keyStorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

TLS/SSL Keystore File Password

Description

The password for the Navigator Metadata Server keystore file.

Related Name

nav.ssl.keyStorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Parameter Validation: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Navigator Metadata Server Storage Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Storage Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_data_dir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Navigator Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Navigator Metadata Server Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Navigator Metadata Server Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: HDFS Filter Blacklist

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the HDFS Filter Blacklist parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_filter_hdfs_rules

Required

true

Suppress Parameter Validation: S3 Filter list

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the S3 Filter list parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_filter_s3_rules

Required

true

Suppress Parameter Validation: Navigator Kerberos Principal for HDFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Kerberos Principal for HDFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_hdfs_kerberos_princ

Required

true

Suppress Parameter Validation: Navigator Metadata Server Install Dir

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Install Dir parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_install_dir

Required

true

Suppress Parameter Validation: LDAP Bind User Distinguished Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind User Distinguished Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_bind_dn

Required

true

Suppress Parameter Validation: LDAP Bind Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Bind Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_bind_pw

Required

true

Suppress Parameter Validation: LDAP Distinguished Name Pattern

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Distinguished Name Pattern parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_dn_pattern

Required

true

Suppress Parameter Validation: LDAP Group Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_group_search_base

Required

true

Suppress Parameter Validation: LDAP Group Search Filter For Logged In User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Group Search Filter For Logged In User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_group_search_filter

Required

true

Suppress Parameter Validation: LDAP Groups Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP Groups Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_groups_search_filter

Required

true

Suppress Parameter Validation: LDAP URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_url

Required

true

Suppress Parameter Validation: LDAP User Search Base

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Search Base parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_user_search_base

Required

true

Suppress Parameter Validation: LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the LDAP User Search Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_user_search_filter

Required

true

Suppress Parameter Validation: Navigator Metadata Server Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Database Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_host

Required

true

Suppress Parameter Validation: Navigator Metadata Server Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_name

Required

true

Suppress Parameter Validation: Navigator Metadata Server Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_password

Required

true

Suppress Parameter Validation: Navigator Metadata Server Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Database Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_user

Required

true

Suppress Parameter Validation: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Active Directory Domain parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_nt_domain

Required

true

Suppress Parameter Validation: JMS Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMS Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_password

Required

true

Suppress Parameter Validation: JMS Queue

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMS Queue parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_queue

Required

true

Suppress Parameter Validation: JMS URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMS URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_url

Required

true

Suppress Parameter Validation: JMS User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMS User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_user

Required

true

Suppress Parameter Validation: SAML Entity Base URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Entity Base URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_entity_base_url

Required

true

Suppress Parameter Validation: SAML Entity ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Entity ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_entity_id

Required

true

Suppress Parameter Validation: Alias of SAML Sign/Encrypt Private Key

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Alias of SAML Sign/Encrypt Private Key parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_key_alias

Required

true

Suppress Parameter Validation: SAML Sign/Encrypt Private Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Sign/Encrypt Private Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_key_password

Required

true

Suppress Parameter Validation: SAML Keystore Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Keystore Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_keystore_password

Required

true

Suppress Parameter Validation: Path to SAML Keystore File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML Keystore File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_keystore_path

Required

true

Suppress Parameter Validation: SAML Login URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Login URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_login_url

Required

true

Suppress Parameter Validation: Path to SAML IDP Metadata File

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML IDP Metadata File parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_metadata_path

Required

true

Suppress Parameter Validation: SAML Attribute Identifier for User Role

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Attribute Identifier for User Role parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_oid_role

Required

true

Suppress Parameter Validation: SAML Attribute Identifier for User ID

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Attribute Identifier for User ID parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_oid_user

Required

true

Suppress Parameter Validation: SAML Attribute Values for Roles

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the SAML Attribute Values for Roles parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_role_map

Required

true

Suppress Parameter Validation: Path to SAML Role Assignment Script

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Path to SAML Role Assignment Script parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_role_script

Required

true

Suppress Parameter Validation: Default Facets

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Default Facets parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_search_default_facets

Required

true

Suppress Parameter Validation: Cloudera Telemetry Publisher S3 Bucket

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Telemetry Publisher S3 Bucket parameter.

Related Name

Default Value

false

API Name

role_config_suppression_nav_telemetry_bucket_name

Required

true

Suppress Parameter Validation: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Audit Event Filter parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_audit_event_filter

Required

true

Suppress Parameter Validation: Navigator Metadata Server Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Parameter Validation: Java Configuration Options for Navigator Metadata Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Navigator Metadata Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_java_opts

Required

true

Suppress Parameter Validation: Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_safety_valve

Required

true

Suppress Parameter Validation: Navigator Metadata Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_server_port

Required

true

Suppress Parameter Validation: Navigator Metadata Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Navigator Metadata Server Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_navigatormetaserver_role_env_safety_valve

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: TLS/SSL Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: TLS/SSL Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: TLS/SSL Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Log Directory Free Space

Description

Whether to suppress the results of the Audit Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_audit_event_log_directory_free_space

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_audit_health

Required

true

Suppress Health Test: Navigator Metadata Server Storage Dir Free Space

Description

Whether to suppress the results of the Navigator Metadata Server Storage Dir Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_data_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_navigatormetaserver_unexpected_exits

Required

true

Suppress Health Test: Solr Element Count Threshold Test

Description

Whether to suppress the results of the Solr Element Count Threshold Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nms_solr_element_count

Required

true

Suppress Health Test: Solr Relation Count Threshold Test

Description

Whether to suppress the results of the Solr Relation Count Threshold Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_nms_solr_relation_count

Required

true

Reports Manager

Advanced

Java Configuration Options for Reports Manager

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

headlamp_java_opts

Required

false

Maximum Document Buffer Size

Description

Amount of memory that can be used for buffering documents before they are flushed to the index. For faster indexing performance, consider increasing this value.

Related Name

lucene.max.buffer.size.mb

Default Value

32 MiB

API Name

headlamp_lucene_max_buffer_size_mb

Required

false

Index Merge Factor

Description

Reports Manager index is built in sections that are merged as the build progresses. This configuration determines how often index sections are merged. With smaller values, less memory is used while indexing, but indexing speed is slower. For faster indexing performance, consider increasing this value.

Related Name

lucene.merge.factor

Default Value

100

API Name

headlamp_lucene_merge_factor

Required

false

Publish HBase Space Usage

Description

When set, publishes HBase space usage metrics to support HBase usage reporting. This feature is only supported for the HBase service in CDH 5 and higher.

Related Name

publish.hbase.space

Default Value

true

API Name

headlamp_publish_hbase_metrics

Required

false

Enable snapshot processing

Description

When set, the HDFS snapshots will be processed and their size will appear in the HDFS Usage reports. Enabling this feature can cause huge memory consumption in the Reports Manager.

Related Name

snapshot.processing.enabled

Default Value

false

API Name

headlamp_snapshot_processing_enabled

Required

false

Reports Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.db.properties

Description

For advanced use only. A string to be inserted into headlamp.db.properties for this role only.

Related Name

Default Value

API Name

reportsmanager_db_safety_valve

Required

false

Reports Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

REPORTSMANAGER_role_env_safety_valve

Required

false

Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.conf

Description

For advanced use only. A string to be inserted into headlamp.conf for this role only.

Related Name

Default Value

API Name

reportsmanager_safety_valve

Required

false

Database

Reports Manager Database Hostname

Description

Name of the host where Reports Manager's database is running. It is highly recommended that this database is on the same host as Reports Manager. If the database is not running on its default port, specify the port number using this syntax: 'host:port'

Related Name

com.cloudera.headlamp.db.host

Default Value

localhost

API Name

headlamp_database_host

Required

false

Reports Manager Database Name

Description

The name of the Reports Manager's database.

Related Name

com.cloudera.headlamp.db.name

Default Value

headlamp

API Name

headlamp_database_name

Required

true

Reports Manager Database Password

Description

The password for Reports Manager's database user account.

Related Name

com.cloudera.headlamp.db.password

Default Value

API Name

headlamp_database_password

Required

false

Reports Manager Database Type

Description

Type of database used for Reports Manager.

Related Name

com.cloudera.headlamp.db.type

Default Value

mysql

API Name

headlamp_database_type

Required

false

Reports Manager Database Username

Description

The username to use to log into Reports Manager's database.

Related Name

com.cloudera.headlamp.db.user

Default Value

headlamp

API Name

headlamp_database_user

Required

true

Logs

Reports Manager Logging Threshold

Description

The minimum log level for Reports Manager logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Reports Manager Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Reports Manager logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Reports Manager Max Log Size

Description

The maximum size, in megabytes, per log file for Reports Manager logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Reports Manager Log Directory

Description

Directory where Reports Manager will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-headlamp

API Name

mgmt_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for

that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following

configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

reportsmanager_fd_thresholds

Required

false

Reports Manager Host Health Test

Description

When computing the overall Reports Manager health, consider the host's health.

Related Name

Default Value

true

API Name

reportsmanager_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

reportsmanager_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

reportsmanager_pause_duration_window

Required

false

Reports Manager Process Health Test

Description

Enables the health test that the Reports Manager's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

reportsmanager_scm_health_enabled

Required

false

Reports Manager Working Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Reports Manager Working Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

reportsmanager_scratch_directory_free_space_absolute_thresholds

Required

false

Reports Manager Working Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Reports Manager Working Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Reports Manager Working Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

reportsmanager_scratch_directory_free_space_percentage_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.

- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

scm_descriptor_age_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Reports Manager Working Directory

Description

Directory for Reports Manager to use for its working files

Related Name

scratch.dir

Default Value

/var/lib/cloudera-scm-headlamp

API Name

headlamp_scratch_dir

Required

false

Reports Manager Update Frequency

Description

Frequency in which Reports Manager refreshes its view of HDFS.

Related Name

update.frequency.seconds

Default Value

1 hour(s)

API Name

headlamp_update_frequency_seconds

Required

false

Starting Interval for Descriptor Fetch Attempts

Description

The starting interval between fetch attempts for the SCM descriptor when Cloudera Management Service roles are starting. The interval is increased by an additional one second with each failed fetch attempt.

Related Name

mgmt.descriptor.fetch.frequency

Default Value

2 second(s)

API Name

mgmt_descriptor_fetch_frequency

Required

true

Descriptor Fetch Max Attempts

Description

Maximum number of attempts to fetch the SCM descriptor when Cloudera Management Service roles are starting. If the roles are not able to get the descriptor in this number of attempts, then the roles exit.

Related Name

mgmt.num.descriptor.fetch.tries

Default Value

10

API Name

mgmt_num_descriptor_fetch_tries

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Bind Reports Manager to Wildcard Address

Description

If enabled, the Reports Manager binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

headlamp_bind_wildcard

Required

false

Reports Manager Web UI Port

Description

The port where Reports Manager starts a debug web server. Set to -1 to disable debug server.

Related Name

debug.server.port

Default Value

8083

API Name

headlamp_debug_port

Required

false

Reports Manager Server Port

Description

The port where Reports Manager listens for requests

Related Name

server.port

Default Value

5678

API Name

headlamp_server_port

Required

false

Resource Management

Java Heap Size of Reports Manager in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

headlamp_heapsize

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Reports Manager Kerberos Principal

Description

Kerberos principal used by Reports Manager. Note: This principal must have administrator and superuser privileges on all HDFS services.

Related Name

Default Value

hdfs

API Name

kerberos_role_princ_name

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Reports Manager Database Hostname

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Database Hostname parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_host

Required

true

Suppress Parameter Validation: Reports Manager Database Name

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Database Name parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_name

Required

true

Suppress Parameter Validation: Reports Manager Database Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Database Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_password

Required

true

Suppress Parameter Validation: Reports Manager Database Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Database Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_user

Required

true

Suppress Parameter Validation: Reports Manager Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_debug_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Reports Manager

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Reports Manager parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_java_opts

Required

true

Suppress Parameter Validation: Reports Manager Working Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Working Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_scratch_dir

Required

true

Suppress Parameter Validation: Reports Manager Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_server_port

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Reports Manager Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Reports Manager Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Reports Manager Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.db.properties

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.db.properties parameter.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_db_safety_valve

Required

true

Suppress Parameter Validation: Reports Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_role_env_safety_valve

Required

true

Suppress Parameter Validation: Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_safety_valve

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_pause_duration

Required

true

Suppress Health Test: Cloudera Manager Descriptor Age

Description

Whether to suppress the results of the Cloudera Manager Descriptor Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_scm_descriptor_fetch

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_scm_health

Required

true

Suppress Health Test: Reports Manager Working Directory Free Space

Description

Whether to suppress the results of the Reports Manager Working Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_scratch_directory_free_space

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_reports_manager_unexpected_exits

Required

true

Service Monitor

Advanced

Java Configuration Options for Service Monitor

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

firehose_java_opts

Required

false

Service Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

For advanced use only. A string to be inserted into cmon.conf for this role only.

Related Name

Default Value

API Name

firehose_safety_valve

Required

false

Service Monitor Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Service Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

SERVICEMONITOR_role_env_safety_valve

Required

false

Event Publication Maximum Queue Size

Description

The maximum size of the queue in which events published from this role will be buffered. If this queue becomes full (for example, due to an outage), subsequent events will be dropped.

Related Name

health.event.publish.queue.max

Default Value

20000

API Name

svcmon_event_publication_queue_size_max

Required

true

Event Publication Retry Period

Description

If an event cannot be delivered immediately by this role, this value controls how long to wait before Event Publisher retries delivery.

Related Name

health.event.publish.retry.ms

Default Value

5000

API Name

svcmon_event_publication_retry_period

Required

true

Logs

Service Monitor Logging Threshold

Description

The minimum log level for Service Monitor logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Service Monitor Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Service Monitor logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Service Monitor Max Log Size

Description

The maximum size, in megabytes, per log file for Service Monitor logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Service Monitor Log Directory

Description

Location of log files for Service Monitor

Related Name

Default Value

/var/log/cloudera-scm-firehose

API Name

mgmt_log_dir

Required

false

Monitoring

Metrics Aggregation Run Duration Thresholds

Description

The health test thresholds for monitoring the metrics aggregation run duration.

Related Name

Default Value

Warning: 10 second(s), Critical: 30 second(s)

API Name

aggregation_run_duration_thresholds

Required

false

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Service Monitor Storage Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Service Monitor Storage Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

firehose_storage_directory_free_space_absolute_thresholds

Required

false

Service Monitor Storage Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Service Monitor Storage Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Service Monitor Storage Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

firehose_storage_directory_free_space_percentage_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Cloudera Manager Metric Schema Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager metric schema was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

metric_schema_age_thresholds_name

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following configuration enables the collection of metrics required for Health Tests and the jvm_heap_use d_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

receivers: prometheus/$ROLE_NAME: config: scrape_configs: - job_name: 'cm_direct' scheme: $ROLE_BOOLEAN_PARAM(ssl_enabled, 'https', 'http') static_configs: - targets: ['localhost:$ROLE_PARAM(prometheus_metrics_endpoint_port)'] labels: $DECODE_URL($SYS_PARAM(com.cloudera.cmf.otelcol.labels.urlencoded)) basic_auth: username: $ROLE_PARAM(prometheus_metrics_endpoint_username) password: $ROLE_PARAM(prometheus_metrics_endpoint_password) tls_config: insecure_skip_verify: true

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

service: pipelines: metrics/$ROLE_NAME: receivers: [prometheus/$ROLE_NAME] exporters: [prometheusremotewrite/$ROLE_NAME]

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.

- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Cloudera Manager Descriptor Age Thresholds

Description

The health test thresholds for monitoring the time since the Cloudera Manager descriptor was last refreshed.

Related Name

Default Value

Warning: 60000.0, Critical: 120000.0

API Name

scm_descriptor_age_thresholds

Required

false

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

servicemonitor_fd_thresholds

Required

false

Heap Size Thresholds

Description

The health test thresholds for the heap used.

Related Name

Default Value

Warning: 90.0 %, Critical: 95.0 %

API Name

servicemonitor_heap_size_thresholds

Required

false

Service Monitor Host Health Test

Description

When computing the overall Service Monitor health, consider the host's health.

Related Name

Default Value

true

API Name

servicemonitor_host_health_enabled

Required

false

Pause Duration Thresholds

Description

The health test thresholds for the weighted average extra time the pause monitor spent paused. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

servicemonitor_pause_duration_thresholds

Required

false

Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

Default Value

5 minute(s)

API Name

servicemonitor_pause_duration_window

Required

false

Service Monitor Role Pipeline Monitoring Thresholds

Description

The health test thresholds for monitoring the Service Monitor role pipeline. This specifies the number of dropped messages that will be tolerated over the monitoring time period.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

servicemonitor_role_pipeline_thresholds

Required

false

Service Monitor Role Pipeline Monitoring Time Period

Description

The time period over which the Service Monitor role pipeline will be monitored for dropped messages.

Related Name

Default Value

5 minute(s)

API Name

servicemonitor_role_pipeline_window

Required

false

Service Monitor Process Health Test

Description

Enables the health test that the Service Monitor's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

servicemonitor_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

servicemonitor_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

servicemonitor_web_metric_collection_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

YARN MapReduce Counter Descriptions

Description

This JSON document contains metadata that is used by the Service Monitor's YARN application monitoring feature for YARN-based MapReduce counter handling. Each counter description has the following fields:

- name (mandatory) - the name of the counter, for example, org.apache.hadoop.mapreduce.filesystemcounter.file_bytes_read.

- units (mandatory) - the units of the counter.
- attributeName (optional) - the attribute name to use for the counter within Cloudera Manager, this name will be used to identify the counter within the YARN Application Monitoring feature and in the Cloudera Manager API. If not specified the portion of the counter name after the last period will be used.
- displayName (optional) - a display name for the counter. If not specified the full counter name will be used.
- description (optional) - a description of the counter. If not specified the full counter name will be used.

Related Name

Default Value

[name: org.apache.hadoop.mapreduce.jobcounter.num_failed_maps, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.num_failed_reduces, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.total_launched_maps, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.total_launched_reduces, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.other_local_maps, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.data_local_maps, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.rack_local_maps, units: tasks , name: org.apache.hadoop.mapreduce.jobcounter.slots_millis_maps, units: ms , name: org.apache.hadoop.mapreduce.jobcounter.slots_millis_reduces, units: ms , name: org.apache.hadoop.mapreduce.jobcounter.fallow_slots_millis_maps, units: ms , name: org.apache.hadoop.mapreduce.jobcounter.fallow_slots_millis_reduces, units: ms , name: org.apache.hadoop.mapreduce.jobcounter.mb_millis_maps, units: mb millis , name: org.apache.hadoop.mapreduce.jobcounter.mb_millis_reduces, units: mb millis , name: org.apache.hadoop.mapreduce.jobcounter.vcores_millis_maps, units: vcore millis , name: org.apache.hadoop.mapreduce.jobcounter.vcores_millis_reduces, units: vcore millis , name: org.apache.hadoop.mapreduce.filesystemcounter.file_bytes_read, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.file_bytes_written, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.file_read_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.file_large_read_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.file_write_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.hdfs_bytes_read, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.hdfs_bytes_written, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.hdfs_read_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.hdfs_large_read_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.hdfs_write_ops, units: operations , name: org.apache.hadoop.mapreduce.filesystemcounter.s3a_bytes_read, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.s3a_bytes_written, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.adl_bytes_read, units: bytes , name: org.apache.hadoop.mapreduce.filesystemcounter.adl_bytes_written, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.map_input_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.map_output_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.map_output_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.map_output_materialized_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.split_raw_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.combine_input_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.combine_output_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.reduce_input_groups, units: groups , name: org.apache.hadoop.mapreduce.taskcounter.reduce_shuffle_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.reduce_input_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.reduce_output_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.spilled_records, units: records , name: org.apache.hadoop.mapreduce.taskcounter.shuffled_maps, units: tasks , name: org.apache.hadoop.mapreduce.taskcounter.failed_shuffle, units:

failures , name: org.apache.hadoop.mapreduce.taskcounter.merged_map_outputs, units: outputs , name: org.apache.hadoop.mapreduce.taskcounter.gc_time_millis, units: ms , name: org.apache.hadoop.mapreduce.taskcounter.cpu_milliseconds, units: ms , name: org.apache.hadoop.mapreduce.taskcounter.physical_memory_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.virtual_memory_bytes, units: bytes , name: org.apache.hadoop.mapreduce.taskcounter.committed_heap_bytes, units: bytes , attributeName: shuffle_errors_bad_id, name: shuffle_errors.bad_id, units: errors , attributeName: shuffle_errors_connection, name: shuffle_errors.connection, units: errors , attributeName: shuffle_errors_io, name: shuffle_errors.io_error, units: errors , attributeName: shuffle_errors_wrong_length, name: shuffle_errors.wrong_length, units: errors , attributeName: shuffle_errors_wrong_map, name: shuffle_errors.wrong_map, units: errors , attributeName: shuffle_errors_wrong_reduce, name: shuffle_errors.wrong_reduce, units: errors , name: org.apache.hadoop.mapreduce.lib.input.fileinputformatcounter.bytes_read, units: bytes , name: org.apache.hadoop.mapreduce.lib.output.fileoutputformatcounter.bytes_written, units: bytes]

API Name

yarn_application_mapreduce_counters

Required

false

Other

Use the Authentication Service to enable Single Sign On

Description

Use the Authentication Service to enable Single Sign On for the Firehose debug servers. Requires a running Authentication Service.

Related Name

debug.servlet.auth.enabled

Default Value

false

API Name

debug_servlet_auth_enabled

Required

false

Impala Storage

Description

The approximate amount of disk space dedicated to storing Impala query data. Once the store has reached its maximum size, older data is deleted to make room for newer queries. The disk usage is approximate because data is deleted only when the limit is reached.

Related Name

firehose_impala_storage_bytes

Default Value

1 GiB

API Name

firehose_impala_storage_bytes

Required

false

Reports Time-series Storage

Description

The approximate amount of disk space dedicated to storing time series for reporting data. Once the store has reached its maximum size, older data is deleted to make room for newer data. The disk usage is approximate because data is deleted only when the limit is reached. See the "Disk Usage" tab on the Service Monitor page for more information on how space is consumed in the Service Monitor. This tab also shows information about the amount of data retained and the time window covered by each data granularity.

Related Name

firehose_reports_storage_bytes

Default Value

1 GiB

API Name

firehose_reports_storage_bytes

Required

false

Service Monitor Storage Directory

Description

The directory where Service Monitor data is stored. The Service Monitor stores metric time series and health information, as well as Impala query and YARN application metadata if Impala and/or YARN are configured.

Related Name

firehose.storage.base.directory

Default Value

/var/lib/cloudera-service-monitor

API Name

firehose_storage_dir

Required

true

Time-Series Storage

Description

The approximate amount of disk space dedicated to storing time series and health data. Once the store has reached its maximum size, older data is deleted to make room for newer data. The disk usage is approximate because data is deleted only when the limit is reached.Note that Cloudera Manager stores time-series data at a number of different data granularities, and these granularities have different effective retention periods. Specifically, Cloudera Manager stores metric data as both raw data points and ten-minutely, hourly, six-hourly, daily, and weekly summary data points. Raw data consumes the bulk of the allocated storage space, weekly summaries the least. As such, raw data is retained for the shortest amount of time, while weekly summary points are unlikely to ever be deleted.See the "Storage" tab on the 'Service Monitor' -> 'Charts Library' -> 'Service Monitor Storage' page for more information on how space is consumed within the Service Monitor. This tab also shows information about the amount of data retained and time window covered by each data granularity.

Related Name

firehose_time_series_storage_bytes

Default Value

10 GiB

API Name

firehose_time_series_storage_bytes

Required

false

YARN Storage

Description

The approximate amount of disk space dedicated to storing YARN application data. Once the store has reached its maximum size, older data is deleted to make room for newer applications. The disk usage is approximate because data is deleted only when the limit is reached.

Related Name

firehose_yarn_storage_bytes

Default Value

1 GiB

API Name

firehose_yarn_storage_bytes

Required

false

Health Event Startup Policy

Description

This setting controls whether health events are emitted when this monitoring role is started. If set to "none", then no health events are emitted. If set to "bad" then health events are emitted for subjects with bad or concerning health. If set to "all" then health events are emitted for all subjects for all health values. The default is "bad".

Related Name

health.event.publish.startup.policy

Default Value

bad

API Name

health_event_publish_startup_policy

Required

false

Starting Interval for Descriptor Fetch Attempts

Description

The starting interval between fetch attempts for the SCM descriptor when Cloudera Management Service roles are starting. The interval is increased by an additional one second with each failed fetch attempt.

Related Name

mgmt.descriptor.fetch.frequency

Default Value

2 second(s)

API Name

mgmt_descriptor_fetch_frequency

Required

true

Descriptor Fetch Max Attempts

Description

Maximum number of attempts to fetch the SCM descriptor when Cloudera Management Service roles are starting. If the roles are not able to get the descriptor in this number of attempts, then the roles exit.

Related Name

mgmt.num.descriptor.fetch.tries

Default Value

10

API Name

mgmt_num_descriptor_fetch_tries

Required

true

Prometheus adapter configuration

Description

JSON configuration specifying metrics to expose on the experimental Prometheus-compatible endpoint, if enabled.

Related Name

prometheus.adapter.config

Default Value

[subject_type: HBASE-MASTER, metrics: [jvm_gc_rate, jvm_gc_time_ms_rate, jvm_max_memory_mb, jvm_heap_committed_mb, jvm_heap_used_mb, jvm_non_heap_committed_mb, jvm_non_heap_used_mb, jvm_total_threads, jvm_blocked_threads, jvm_new_threads, jvm_runnable_threads, jvm_terminated_threads, jvm_timed_waiting_threads, jvm_waiting_threads, gc_count_concurrent_mark_sweep_rate, gc_count_par_new_rate, gc_time_ms_concurrent_mark_sweep_rate, gc_time_ms_par_new_rate, ipc_process_rate, ipc_process_time_75th_percentile, ipc_process_time_95th_percentile, ipc_process_time_99th_percentile, ipc_process_time_max, ipc_process_time_mean, ipc_process_time_median, ipc_process_time_min, ipc_queue_rate, ipc_queue_time_75th_percentile, ipc_queue_time_95th_percentile, ipc_queue_time_99th_percentile, ipc_queue_time_max, ipc_queue_time_mean, ipc_queue_time_median, ipc_queue_time_min, ipc_received_bytes_Rate, ipc_sent_bytes_Rate, get_hadoop_groups_avg_time, get_hadoop_groups_rate, assign_rate, regions_in_transition_over_threshold, regions_in_transition_longest_time, regions_in_transition, bulk_assign_rate, balance_cluster_rate, balance_cluster_max, balance_cluster_median, balance_cluster_99th_percentile, balance_cluster_mean, balance_cluster_75th_percentile, balance_cluster_min, balance_cluster_95th_percentile, balancer_misc_invocations, master_start_time, master_active_time, regionservers, dead_regionservers, bulk_assign_mean, assign_95th_percentile, assign_min, assign_75th_percentile, bulk_assign_max, bulk_assign_min, assign_median, bulk_assign_95th_percentile, bulk_assign_median, assign_max, assign_mean, bulk_assign_75th_percentile, assign_99th_percentile, bulk_assign_99th_percentile, orphan_regions_on_regionserver, audit_agent_bytes_left_rate, audit_agent_send_failures_rate, audit_plugin_coalesced_rate, audit_plugin_events_rate, audit_plugin_exceptions_rate, audit_plugin_filtered_rate, audit_plugin_parse_errors_rate, log_error_rate, log_fatal_rate, log_warn_rate, login_failure_avg_time, login_failure_rate, login_success_rate, metrics_dropped_pub_all, metrics_num_active_sinks, metrics_num_active_sources, metrics_num_all_sinks, metrics_num_all_sources,

metrics_publish_avg_time, metrics_publish_rate, metrics_snapshot_avg_time, metrics_snapshot_rate, ipc_authentication_failures_rate, ipc_authentication_successes_rate, ipc_authorization_failures_rate, ipc_authorization_successes_rate, orphan_regions_on_filesystem, inconsistent_regions, region_holes, region_overlaps, unknown_server_regions, empty_region_info_regions] , subject_type: HBASE-REGIONSERVER, metrics: [jvm_gc_rate, jvm_gc_time_ms_rate, jvm_max_memory_mb, jvm_heap_committed_mb, jvm_heap_used_mb, jvm_non_heap_committed_mb, jvm_non_heap_used_mb, jvm_total_threads, jvm_blocked_threads, jvm_new_threads, jvm_runnable_threads, jvm_terminated_threads, jvm_timed_waiting_threads, jvm_waiting_threads, slow_append_rate, slow_delete_rate, slow_get_rate, slow_increment_rate, slow_put_rate, pause_time_with_gc_99_9th_percentile, pause_time_with_gc_mean, pause_time_with_gc_rate, pause_time_without_gc_99_9th_percentile, pause_time_without_gc_mean, pause_time_without_gc_rate, gc_count_concurrent_mark_sweep_rate, gc_count_par_new_rate, gc_time_ms_concurrent_mark_sweep_rate, gc_time_ms_par_new_rate, ipc_process_rate, ipc_process_time_75th_percentile, ipc_process_time_95th_percentile, ipc_process_time_99th_percentile, ipc_process_time_max, ipc_process_time_mean, ipc_process_time_median, ipc_process_time_min, ipc_queue_rate, ipc_queue_time_75th_percentile, ipc_queue_time_95th_percentile, ipc_queue_time_99th_percentile, ipc_queue_time_max, ipc_queue_time_mean, ipc_queue_time_median, ipc_queue_time_min, ipc_received_bytes_rate, ipc_sent_bytes_rate, block_cache_blocks_cached, block_cache_evicted_rate, block_cache_express_hit_ratio, block_cache_free_size, block_cache_hit_rate, block_cache_hit_ratio, block_cache_miss_rate, block_cache_size, append_75th_percentile, append_95th_percentile, append_99th_percentile, append_max, append_mean, append_median, append_min, append_rate, delete_median, delete_min, delete_max, delete_rate, get_75th_percentile, get_95th_percentile, get_99th_percentile, get_hadoop_groups_avg_time, get_hadoop_groups_rate, get_max, get_mean, get_median, get_min, wal_append_time_75th_percentile, wal_append_time_95th_percentile, wal_append_time_99th_percentile, wal_append_time_max, wal_append_time_mean, wal_append_time_median, wal_append_time_min, wal_append_size_mean, wal_append_size_median, wal_append_size_min, wal_append_rate, wal_append_size_75th_percentile, wal_append_size_95th_percentile, wal_append_size_99th_percentile, wal_append_size_max, scan_time_max, scan_time_mean, scan_time_median, scan_time_min, scan_time_rate, scan_size_75th_percentile, scan_size_95th_percentile, scan_size_99th_percentile, scan_size_max, scan_size_mean, scan_size_median, scan_size_min, scan_size_rate, increment_75th_percentile, increment_95th_percentile, increment_99th_percentile, increment_max, increment_mean, increment_median, increment_min, increment_rate, delete_75th_percentile, delete_95th_percentile, delete_99th_percentile, delete_max, delete_mean, wal_sync_time_99th_percentile, wal_sync_time_max, wal_sync_time_mean, wal_sync_time_median, wal_sync_time_min, mutate_rate, mutations_without_wal_rate, mutations_without_wal_size, check_mutate_failed_rate, check_mutate_passed_rate, get_rate, num_puts_without_wal, read_requests_rate, replay_75th_percentile, replay_95th_percentile, replay_99th_percentile, replay_max, replay_mean, replay_median, replay_min, replay_rate, regions, regionserver_start_time, slave_master_connectivity, percent_hfiles_local, static_bloom_size, static_index_size, storefile_index_size, storefiles, storefiles_size, stores, requests_rate, updates_blocked_time_rate, compaction_queue_size, flush_queue_size, audit_agent_bytes_left_rate, audit_agent_send_failures_rate, audit_plugin_coalesced_rate, audit_plugin_events_rate, audit_plugin_exceptions_rate, audit_plugin_filtered_rate, audit_plugin_parse_errors_rate, log_error_rate, log_fatal_rate, log_warn_rate, login_failure_avg_time, login_failure_rate, login_success_rate, memstore_size, metrics_dropped_pub_all, metrics_num_active_sinks, metrics_num_active_sources, metrics_num_all_sinks, metrics_num_all_sources, metrics_publish_avg_time, metrics_publish_rate, metrics_snapshot_avg_time, metrics_snapshot_rate, ipc_authentication_failures_rate, ipc_authentication_successes_rate, ipc_authorization_failures_rate, ipc_authorization_successes_rate] , subject_type: HIVE_ON_TEZ-HIVESERVER2, metrics: [hive_memory_heap_used, hive_memory_non_heap_used, mem_rss, hive_open_connections, hive_open_operations, hive_waiting_compile_ops, oom_exits_rate,

unexpected_exits_rate, hive_jvm_pause_time_rate, hive_jvm_pauses_info_threshold_rate, hive_jvm_pauses_warn_threshold_rate] , subject_type: HIVE-HIVEMETASTORE, metrics: [hive_memory_heap_used, hive_memory_non_heap_used, hive_jvm_pause_time_rate, hive_jvm_pauses_info_threshold_rate, hive_jvm_pauses_warn_threshold_rate, hive_open_connections, unexpected_exits_rate, mem_rss] , subject_type: IMPALA-IMPALAD, metrics: [impala_num_queries_registered] , subject_type: RANGER-RANGER_ADMIN, metrics: [mem_rss, oom_exits_rate, unexpected_exits_rate] , subject_type: RANGER-RANGER_TAGSYNC, metrics: [mem_rss, oom_exits_rate, unexpected_exits_rate] , subject_type: RANGER-RANGER_USERSYNC, metrics: [mem_rss, oom_exits_rate, unexpected_exits_rate] , subject_type: RANGER_RAZ-RANGER_RAZ_SERVER, metrics: [mem_rss, oom_exits_rate, unexpected_exits_rate]]

API Name

prometheus_adapter_config

Required

false

Enable Prometheus adapter service

Description

Show a selected subset of metrics from the monitoring subsystem of Cloudera Manager on the experimental Prometheus-compatible metrics endpoint.

Related Name

prometheus.adapter.enabled

Default Value

false

API Name

prometheus_adapter_enabled

Required

true

Event Publication Log Quiet Time Period

Description

To avoid producing excessive amounts of log output, the Event Publisher component of this role is limited to emitting one message per time period. This value controls the size of that time period.

Related Name

health.event.publish.log.suppress.window.ms

Default Value

1 minute(s)

API Name

svcmon_event_publication_log_suppress_window

Required

true

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Service Monitor Web UI Port

Description

Port for Service Monitor's Debug page. Set to -1 to disable the debug server.

Related Name

debug.servlet.port

Default Value

8086

API Name

firehose_debug_port

Required

false

Service Monitor Listen Port

Description

Port where Service Monitor is listening for agent messages.

Related Name

firehose.server.port

Default Value

9997

API Name

firehose_listen_port

Required

false

Service Monitor Nozzle Port

Description

Port where Service Monitor's query API is exposed.

Related Name

nozzle.server.port

Default Value

9996

API Name

firehose_nozzle_port

Required

false

Prometheus Metrics Endpoint Port

Description

Port where an experimental Prometheus-compatible metrics endpoint is exposed. Set to -1 to disable the endpoint.

Related Name

prometheus.metrics.endpoint.port

Default Value

-1

API Name

prometheus_metrics_endpoint_port

Required

false

Bind Service Monitor to Wildcard Address

Description

If enabled, the Service Monitor binds to the wildcard address ("0.0.0.0") on all of its ports.

Related Name

Default Value

false

API Name

smon_bind_wildcard

Required

false

Resource Management

Java Heap Size of Service Monitor in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

firehose_heapsize

Required

false

Maximum Non-Java Memory of Service Monitor

Description

The amount of memory the Service Monitor can use off of the Java heap.

Related Name

firehose_non_java_memory_bytes

Default Value

2 GiB

API Name

firehose_non_java_memory_bytes

Required

false

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Security

Role-Specific Kerberos Principal

Description

Kerberos principal used by the Service Monitor roles.

Related Name

Default Value

hue

API Name

kerberos_role_princ_name

Required

true

Prometheus Metrics Endpoint Password

Description

Password for the experimental Prometheus-compatible metrics endpoint. Changes require a restart to take effect.

Related Name

prometheus.metrics.endpoint.password

Default Value

API Name

prometheus_metrics_endpoint_password

Required

false

Prometheus Metrics Endpoint Username

Description

Username for the experimental Prometheus-compatible metrics endpoint. Changes require a restart to take effect.

Related Name

prometheus.metrics.endpoint.username

Default Value

API Name

prometheus_metrics_endpoint_username

Required

false

Enable TLS/SSL for Firehose Debug Server

Description

Encrypt communication between clients and Firehose Debug Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

debug.servlet.https.enabled

Default Value

false

API Name

ssl_enabled

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Firehose Debug Server is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

debug.servlet.https.keystorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Firehose Debug Server TLS/SSL Server Keystore File Password

Description

The password for the Firehose Debug Server keystore file.

Related Name

debug.servlet.https.keystorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: Service Monitor Web UI Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Web UI Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_debug_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Service Monitor

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Service Monitor parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_java_opts

Required

true

Suppress Parameter Validation: Service Monitor Listen Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Listen Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_listen_port

Required

true

Suppress Parameter Validation: Service Monitor Nozzle Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Nozzle Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_nozzle_port

Required

true

Suppress Parameter Validation: Service Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_safety_valve

Required

true

Suppress Configuration Validator: Service Monitor Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Service Monitor Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_service_monitor_heap_role_validator

Required

true

Suppress Configuration Validator: Service Monitor Off Heap Memory Size Validator

Description

Whether to suppress configuration warnings produced by the Service Monitor Off Heap Memory Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_service_monitor_non_java_memory_role_validator

Required

true

Suppress Parameter Validation: Service Monitor Storage Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Storage Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_storage_dir

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role-Specific Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Service Monitor Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Service Monitor Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Prometheus adapter configuration

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus adapter configuration parameter.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_adapter_config

Required

true

Suppress Parameter Validation: Prometheus Metrics Endpoint Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Metrics Endpoint Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_password

Required

true

Suppress Parameter Validation: Prometheus Metrics Endpoint Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Metrics Endpoint Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_port

Required

true

Suppress Parameter Validation: Prometheus Metrics Endpoint Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Prometheus Metrics Endpoint Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_username

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Service Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_servicemonitor_role_env_safety_valve

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Firehose Debug Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Firehose Debug Server TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: YARN MapReduce Counter Descriptions

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the YARN MapReduce Counter Descriptions parameter.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_application_mapreduce_counters

Required

true

Suppress Health Test: Metrics Aggregation Run Duration Test

Description

Whether to suppress the results of the Metrics Aggregation Run Duration Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_aggregation_run_duration

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_audit_health

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_file_descriptor

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_heap_dump_directory_free_space

Required

true

Suppress Health Test: Heap Size

Description

Whether to suppress the results of the Heap Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_heap_size

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_log_directory_free_space

Required

true

Suppress Health Test: Cloudera Manager Metric Schema Age

Description

Whether to suppress the results of the Cloudera Manager Metric Schema Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_metric_schema_fetch

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_otelcol_health

Required

true

Suppress Health Test: Pause Duration

Description

Whether to suppress the results of the Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_pause_duration

Required

true

Suppress Health Test: Role Pipeline

Description

Whether to suppress the results of the Role Pipeline heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_role_pipeline

Required

true

Suppress Health Test: Cloudera Manager Descriptor Age

Description

Whether to suppress the results of the Cloudera Manager Descriptor Age heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_scm_descriptor_fetch

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_scm_health

Required

true

Suppress Health Test: Service Monitor Storage Directory Free Space

Description

Whether to suppress the results of the Service Monitor Storage Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_storage_directory_free_space

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_service_monitor_web_metric_collection

Required

true

Service-Wide

Advanced

Cloudera Management Service Service Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of all roles in this service except client configuration.

Related Name

Default Value

API Name

mgmt_service_env_safety_valve

Required

false

Cloudera Management Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

For advanced use only, a string to be inserted into ssl-client.xml. This setting currently applies to the Reports Manager only.

Related Name

Default Value

API Name

mgmt_ssl_client_safety_valve

Required

false

Small Files Reporting: HDFS Service for Data Staging

Description

Data collection for small files analysis requires a data staging area in HDFS. If you enable data collection for small files reporting, this property sets which HDFS service stages the data.

Related Name

nav.smallfiles.hdfs.staging.service.name

Default Value

API Name

navigator_small_files_staging_hdfs_service_name

Required

false

Small Files Reporting: Enable Data Collection

Description

When Small Files Reporting is enabled, Navigator passes additional metadata to the Telemetry Publisher so the data can be used by Cloudera Workload XM (WXM). This additional data allows WXM to identify Impala query performance issues caused when data is organized into small files in HDFS. Enable this option only when Telemetry Publisher is enabled.

Related Name

nav.smallfiles.reporting.enabled

Default Value

false

API Name

navigator_smallfiles_enabled

Required

true

Small Files Reporting: HDFS Staging Location

Description

Data collection for small files analysis requires a data staging area in HDFS. If you enable data collection for small files reporting, this property sets the HDFS location where Small Files Reporting data is staged. If the directory doesn't already exist, Navigator creates it using the same credentials it uses for HDFS extraction from this service.

Related Name

nav.smallfiles.hdfs.staging.root.path

Default Value

/user/cloudera/navigator/smallfiles

API Name

navigator_smallfiles_hdfs_path

Required

false

System Group

Description

The group that this service's processes should run as.

Related Name

Default Value

cloudera-scm

API Name

process_groupname

Required

true

System User

Description

The user that this service's processes should run as.

Related Name

Default Value

cloudera-scm

API Name

process_username

Required

true

Monitoring

Enable Log Event Capture

Description

When set, each role identifies important log events and forwards them to Cloudera Manager.

Related Name

Default Value

true

API Name

catch_events

Required

false

Enable Service Level Health Alerts

Description

When set, Cloudera Manager will send alerts when the health of this service reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

false

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Cloudera Manager KDC Server Connection Health Thresholds

Description

The health test thresholds for monitoring the KDC Server connection health by login time.

Related Name

Default Value

Warning: 1.5 second(s), Critical: 2 second(s)

API Name

kdc_availability_thresholds

Required

false

KDC Connection Health Check Enabled

Description

Enable or disable Cloudera Manager KDC Server Connection Health Check execution. Restart Cloudera Manager Server to apply changes.

Related Name

Default Value

true

API Name

kdc_monitoring_enabled

Required

false

Cloudera Manager LDAP Server Connection Health Thresholds

Description

The health test thresholds for monitoring the LDAP Server connection health by login time.

Related Name

Default Value

Warning: 1.5 second(s), Critical: 2 second(s)

API Name

ldap_availability_thresholds

Required

false

LDAP Connection Health Check Enabled

Description

Enable or disable Cloudera Manager LDAP Server Connection Health Check execution. Restart Cloudera Manager Server to apply changes.

Related Name

Default Value

true

API Name

ldap_monitoring_enabled

Required

false

Cloudera Manager LDAP Monitoring Period

Description

The Period of the Cloudera Manager's LDAP Monitoring functionality.

Related Name

Default Value

60000

API Name

ldap_monitoring_period

Required

false

Log Event Retry Frequency

Description

The frequency in which the log4j event publication appender will retry sending undelivered log events to the Event server, in seconds

Related Name

Default Value

30

API Name

log_event_retry_frequency

Required

false

Activity Monitor - Unsupported Since 7.0.0 Role Health Test

Description

When computing the overall MGMT health, consider Activity Monitor - Unsupported Since 7.0.0's health

Related Name

Default Value

true

API Name

mgmt_activitymonitor_health_enabled

Required

false

Alert Publisher Role Health Test

Description

When computing the overall MGMT health, consider Alert Publisher's health

Related Name

Default Value

true

API Name

mgmt_alertpublisher_health_enabled

Required

false

Cloudera Manager TLS Certificate Expiry Thresholds

Description

The health test thresholds for monitoring the certificate of Cloudera Manager Server.

Related Name

Default Value

Warning: 60 day(s), Critical: 7 day(s)

API Name

mgmt_certificate_expiry_thresholds

Required

false

Cloudera Manager Server Clock Offset Thresholds

Description

The health test thresholds for monitoring the clock offset between the Cloudera Manager Server and the Service Monitor.

Related Name

Default Value

Warning: 30 second(s), Critical: 1 minute(s)

API Name

mgmt_clock_offset_with_smon_thresholds

Required

false

Cloudera Manager Server Cluster Availability Threshold Percents

Description

The health test thresholds for the Cloudera Manager Server Cluster Availability. Specify the minimum required percent of healthy and running CM cluster nodes.

Related Name

Default Value

Warning: 67.0 %, Critical: 50.0 %

API Name

mgmt_cm_ha_availability_thresholds

Required

false

Command Storage Directory Free Space Monitoring Thresholds

Description

The health test thresholds for monitoring the free space on the filesystem that contains the Cloudera Manager Server command storage directory.

Related Name

Default Value

Warning: 2 GiB, Critical: 1 GiB

API Name

mgmt_command_storage_directory_free_space_absolute_thresholds

Required

false

Embedded Database Free Space Monitoring Thresholds

Description

The health test thresholds for monitoring the free space on the volume for the embedded PostgreSQL database optionally running on the Cloudera Manager Server. If the embedded database is not in use, this has no effect.

Related Name

Default Value

Warning: 2 GiB, Critical: 1 GiB

API Name

mgmt_embedded_database_free_space_absolute_thresholds

Required

false

Event Server Role Health Test

Description

When computing the overall MGMT health, consider Event Server's health

Related Name

Default Value

true

API Name

mgmt_eventserver_health_enabled

Required

false

Cloudera Manager Server Heap Size Thresholds

Description

The health test thresholds for the Cloudera Manager Server heap usage.

Related Name

Default Value

Warning: 90.0 %, Critical: 95.0 %

API Name

mgmt_heap_size_thresholds

Required

false

Host Monitor Role Health Test

Description

When computing the overall MGMT health, consider Host Monitor's health

Related Name

Default Value

true

API Name

mgmt_hostmonitor_health_enabled

Required

false

Navigator Audit Server Role Health Test

Description

When computing the overall MGMT health, consider Navigator Audit Server's health

Related Name

Default Value

true

API Name

mgmt_navigator_health_enabled

Required

false

Navigator Metadata Server Role Health Test

Description

When computing the overall MGMT health, consider Navigator Metadata Server's health

Related Name

Default Value

true

API Name

mgmt_navigatormetaserver_health_enabled

Required

false

Cloudera Manager Server Pause Duration Thresholds

Description

The health test thresholds for the Cloudera Manager Server pause duration time.

Related Name

Default Value

Warning: 2.0 %, Critical: 5.0 %

API Name

mgmt_pause_duration_thresholds

Required

false

Cloudera Manager Server Pause Duration Monitoring Period

Description

The period to review when computing the moving average of extra time the pause monitor spent paused.

Related Name

mgmt.mgmt_pause_duration_window

Default Value

5 minute(s)

API Name

mgmt_pause_duration_window

Required

false

Reports Manager Role Health Test

Description

When computing the overall MGMT health, consider Reports Manager's health

Related Name

Default Value

true

API Name

mgmt_reportsmanager_health_enabled

Required

false

Service Monitor Role Health Test

Description

When computing the overall MGMT health, consider Service Monitor's health

Related Name

Default Value

true

API Name

mgmt_servicemonitor_health_enabled

Required

false

Telemetry Publisher Role Health Test

Description

When computing the overall MGMT health, consider Telemetry Publisher's health

Related Name

Default Value

true

API Name

mgmt_telemetrypublisher_health_enabled

Required

false

Service Triggers

Description

The configured triggers for this service. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific service.
- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger fires if there are more than 10 DataNodes with more than 500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "I F (SELECT fd_open WHERE roleType = DataNode and last(fd_open) > 500) DO health:bad", " streamThreshold": 10, "enabled": "true"}]See the trigger rules documentation for more details on

how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

service_triggers

Required

true

Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a list of derived configuration properties that will be used by the Service Monitor instead of the default ones.

Related Name

Default Value

API Name

smon_derived_configs_safety_valve

Required

false

Other

Emit Sensitive Data In Stderr

Description

If set, sensitive data, like passwords, are emitted to stderr.

Related Name

Default Value

false

API Name

mgmt_emit_sensitive_data_in_stderr

Required

true

Minimum Kerberos Ticket Validity Period

Description

The minimum Kerberos ticket validity period. The Cloudera Management Servies attempt to log in again only after this minimum period of time has elapsed.

Related Name

tgt.login.validity.period

Default Value

1 hour(s)

API Name

tgt_login_validity_period

Required

false

Publishing

Kafka Service

Description

The Kafka service where Navigator will publish audit events.

Related Name

Default Value

API Name

navigator_kafka_publishing_service

Required

false

Security

TLS/SSL Client Truststore File Location

Description

Path to the client truststore file used in HTTPS communication. This truststore contains certificates of trusted servers, or of Certificate Authorities trusted to identify servers. If set, this is used to verify certificates in HTTPS communication with CDH services and the Cloudera Manager Server. If not set, the default Java truststore is used to verify certificates. The contents of this truststore can be modified without restarting the Cloudera Management Service roles. By default, changes to its contents are picked up within ten seconds.

Related Name

ssl.client.truststore.location

Default Value

API Name

ssl_client_truststore_location

Required

false

Cloudera Manager Server TLS/SSL Trust Store Password

Description

The password for the Cloudera Manager Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

Related Name

ssl.client.truststore.password

Default Value

API Name

ssl_client_truststore_password

Required

false

Suppressions

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_activitymonitor_role_env_safety_valve

Required

true

Suppress Configuration Validator: Alert: Mail From Address

Description

Whether to suppress configuration warnings produced by the Alert: Mail From Address configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_from_address

Required

true

Suppress Configuration Validator: Alerts: Mail Server Hostname

Description

Whether to suppress configuration warnings produced by the Alerts: Mail Server Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_hostname

Required

true

Suppress Configuration Validator: Alerts: Mail Server Password

Description

Whether to suppress configuration warnings produced by the Alerts: Mail Server Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_password

Required

true

Suppress Configuration Validator: Alerts: Mail Server TCP Port

Description

Whether to suppress configuration warnings produced by the Alerts: Mail Server TCP Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_port

Required

true

Suppress Configuration Validator: Alerts: Mail Message Recipients

Description

Whether to suppress configuration warnings produced by the Alerts: Mail Message Recipients configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_recipients

Required

true

Suppress Configuration Validator: Alerts: Mail Server Username

Description

Whether to suppress configuration warnings produced by the Alerts: Mail Server Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_mailserver_username

Required

true

Suppress Configuration Validator: Custom Alert Script

Description

Whether to suppress configuration warnings produced by the Custom Alert Script configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_script_path

Required

true

Suppress Configuration Validator: SNMP Authentication Protocol Pass Phrase

Description

Whether to suppress configuration warnings produced by the SNMP Authentication Protocol Pass Phrase configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_auth_password

Required

true

Suppress Configuration Validator: SNMPv2 Community String

Description

Whether to suppress configuration warnings produced by the SNMPv2 Community String configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_community

Required

true

Suppress Configuration Validator: SNMP Server Engine Id

Description

Whether to suppress configuration warnings produced by the SNMP Server Engine Id configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_security_engineid

Required

true

Suppress Configuration Validator: SNMP NMS Hostname

Description

Whether to suppress configuration warnings produced by the SNMP NMS Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_server_hostname

Required

true

Suppress Configuration Validator: SNMP Server Port

Description

Whether to suppress configuration warnings produced by the SNMP Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_server_port

Required

true

Suppress Configuration Validator: SNMP Security UserName

Description

Whether to suppress configuration warnings produced by the SNMP Security UserName configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alert_snmp_username

Required

true

Suppress Configuration Validator: Alerts: Email footer

Description

Whether to suppress configuration warnings produced by the Alerts: Email footer configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_email_footer

Required

true

Suppress Configuration Validator: Alerts: Email header

Description

Whether to suppress configuration warnings produced by the Alerts: Email header configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_email_header

Required

true

Suppress Configuration Validator: Alerts: Listen Port

Description

Whether to suppress configuration warnings produced by the Alerts: Listen Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_internalapi_port

Required

true

Suppress Configuration Validator: Java Configuration Options for Alert Publisher

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Alert Publisher configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_java_opts

Required

true

Suppress Configuration Validator: Alert Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Alert Publisher Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_role_env_safety_valve

Required

true

Suppress Configuration Validator: Alert Publisher Advanced Configuration Snippet (Safety Valve) for alertpublisher.conf

Description

Whether to suppress configuration warnings produced by the Alert Publisher Advanced Configuration Snippet (Safety Valve) for alertpublisher.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_alertpublisher_safety_valve

Required

true

Suppress Configuration Validator: Audit Log Directory

Description

Whether to suppress configuration warnings produced by the Audit Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_audit_event_log_dir

Required

true

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Configuration Validator: Navigator Metadata Server Storage Dir

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Storage Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_data_dir

Required

true

Suppress Configuration Validator: Event Server Web UI Port

Description

Whether to suppress configuration warnings produced by the Event Server Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_debug_port

Required

true

Suppress Configuration Validator: Event Query Port

Description

Whether to suppress configuration warnings produced by the Event Query Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_http_port

Required

true

Suppress Configuration Validator: Event Server Index Directory

Description

Whether to suppress configuration warnings produced by the Event Server Index Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_index_dir

Required

true

Suppress Configuration Validator: Java Configuration Options for Event Server

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Event Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_java_opts

Required

true

Suppress Configuration Validator: Event Publish Port

Description

Whether to suppress configuration warnings produced by the Event Publish Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_listen_port

Required

true

Suppress Configuration Validator: Event Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Event Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: Event Server Advanced Configuration Snippet (Safety Valve) for eventserver.conf

Description

Whether to suppress configuration warnings produced by the Event Server Advanced Configuration Snippet (Safety Valve) for eventserver.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_eventserver_safety_valve

Required

true

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Database Hostname

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Database Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_host

Required

true

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Database Name

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_name

Required

true

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Database Password

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_password

Required

true

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Database Username

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Database Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_database_user

Required

true

Suppress Configuration Validator: Service Monitor Web UI Port

Description

Whether to suppress configuration warnings produced by the Service Monitor Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_debug_port

Required

true

Suppress Configuration Validator: Host Monitor Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Host Monitor Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_host_monitor_heap_role_validator

Required

true

Suppress Configuration Validator: Host Monitor Off Heap Memory Size Validator

Description

Whether to suppress configuration warnings produced by the Host Monitor Off Heap Memory Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_host_monitor_non_java_memory_role_validator

Required

true

Suppress Configuration Validator: Java Configuration Options for Service Monitor

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Service Monitor configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_java_opts

Required

true

Suppress Configuration Validator: Service Monitor Listen Port

Description

Whether to suppress configuration warnings produced by the Service Monitor Listen Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_listen_port

Required

true

Suppress Configuration Validator: Service Monitor Nozzle Port

Description

Whether to suppress configuration warnings produced by the Service Monitor Nozzle Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_nozzle_port

Required

true

Suppress Configuration Validator: Service Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf

Description

Whether to suppress configuration warnings produced by the Service Monitor Advanced Configuration Snippet (Safety Valve) for cmon.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_safety_valve

Required

true

Suppress Configuration Validator: Service Monitor Heap Size Validator

Description

Whether to suppress configuration warnings produced by the Service Monitor Heap Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_service_monitor_heap_role_validator

Required

true

Suppress Configuration Validator: Service Monitor Off Heap Memory Size Validator

Description

Whether to suppress configuration warnings produced by the Service Monitor Off Heap Memory Size Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_service_monitor_non_java_memory_role_validator

Required

true

Suppress Configuration Validator: Service Monitor Storage Directory

Description

Whether to suppress configuration warnings produced by the Service Monitor Storage Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_firehose_storage_dir

Required

true

Suppress Configuration Validator: Reports Manager Database Hostname

Description

Whether to suppress configuration warnings produced by the Reports Manager Database Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_host

Required

true

Suppress Configuration Validator: Reports Manager Database Name

Description

Whether to suppress configuration warnings produced by the Reports Manager Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_name

Required

true

Suppress Configuration Validator: Reports Manager Database Password

Description

Whether to suppress configuration warnings produced by the Reports Manager Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_password

Required

true

Suppress Configuration Validator: Reports Manager Database Username

Description

Whether to suppress configuration warnings produced by the Reports Manager Database Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_database_user

Required

true

Suppress Configuration Validator: Reports Manager Web UI Port

Description

Whether to suppress configuration warnings produced by the Reports Manager Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_debug_port

Required

true

Suppress Configuration Validator: Java Configuration Options for Reports Manager

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Reports Manager configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_java_opts

Required

true

Suppress Configuration Validator: Reports Manager Working Directory

Description

Whether to suppress configuration warnings produced by the Reports Manager Working Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_scratch_dir

Required

true

Suppress Configuration Validator: Reports Manager Server Port

Description

Whether to suppress configuration warnings produced by the Reports Manager Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_headlamp_server_port

Required

true

Suppress Configuration Validator: Host Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Host Monitor Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_hostmonitor_role_env_safety_valve

Required

true

Suppress Configuration Validator: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the JMX Exporter Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Configuration Validator: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the JMX Exporter configuration YAML configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Configuration Validator: Role-Specific Kerberos Principal

Description

Whether to suppress configuration warnings produced by the Role-Specific Kerberos Principal configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Configuration Validator: Service Monitor Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Service Monitor Logging Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Configuration Validator: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the Rules to Extract Events from Log Files configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Configuration Validator: Telemetry Publisher Data Directory

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Data Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_data_dir

Required

true

Suppress Configuration Validator: Service Monitor Log Directory

Description

Whether to suppress configuration warnings produced by the Service Monitor Log Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Configuration Validator: HDFS Filter Blacklist

Description

Whether to suppress configuration warnings produced by the HDFS Filter Blacklist configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_filter_hdfs_rules

Required

true

Suppress Configuration Validator: S3 Filter list

Description

Whether to suppress configuration warnings produced by the S3 Filter list configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_filter_s3_rules

Required

true

Suppress Configuration Validator: Navigator Kerberos Principal for HDFS

Description

Whether to suppress configuration warnings produced by the Navigator Kerberos Principal for HDFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_hdfs_kerberos_princ

Required

true

Suppress Configuration Validator: Navigator Metadata Server Install Dir

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Install Dir configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_install_dir

Required

true

Suppress Configuration Validator: LDAP Bind User Distinguished Name

Description

Whether to suppress configuration warnings produced by the LDAP Bind User Distinguished Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_bind_dn

Required

true

Suppress Configuration Validator: LDAP Bind Password

Description

Whether to suppress configuration warnings produced by the LDAP Bind Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_bind_pw

Required

true

Suppress Configuration Validator: LDAP Distinguished Name Pattern

Description

Whether to suppress configuration warnings produced by the LDAP Distinguished Name Pattern configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_dn_pattern

Required

true

Suppress Configuration Validator: LDAP Group Search Base

Description

Whether to suppress configuration warnings produced by the LDAP Group Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_group_search_base

Required

true

Suppress Configuration Validator: LDAP Group Search Filter For Logged In User

Description

Whether to suppress configuration warnings produced by the LDAP Group Search Filter For Logged In User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_group_search_filter

Required

true

Suppress Configuration Validator: LDAP Groups Search Filter

Description

Whether to suppress configuration warnings produced by the LDAP Groups Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_groups_search_filter

Required

true

Suppress Configuration Validator: LDAP URL

Description

Whether to suppress configuration warnings produced by the LDAP URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_url

Required

true

Suppress Configuration Validator: LDAP User Search Base

Description

Whether to suppress configuration warnings produced by the LDAP User Search Base configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_user_search_base

Required

true

Suppress Configuration Validator: LDAP User Search Filter

Description

Whether to suppress configuration warnings produced by the LDAP User Search Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_ldap_user_search_filter

Required

true

Suppress Configuration Validator: Navigator Metadata Server Database Hostname

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Database Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_host

Required

true

Suppress Configuration Validator: Navigator Metadata Server Database Name

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_name

Required

true

Suppress Configuration Validator: Navigator Metadata Server Database Password

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_password

Required

true

Suppress Configuration Validator: Navigator Metadata Server Database Username

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Database Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_metaserver_database_user

Required

true

Suppress Configuration Validator: Active Directory Domain

Description

Whether to suppress configuration warnings produced by the Active Directory Domain configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_nt_domain

Required

true

Suppress Configuration Validator: JMS Password

Description

Whether to suppress configuration warnings produced by the JMS Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_password

Required

true

Suppress Configuration Validator: JMS Queue

Description

Whether to suppress configuration warnings produced by the JMS Queue configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_queue

Required

true

Suppress Configuration Validator: JMS URL

Description

Whether to suppress configuration warnings produced by the JMS URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_url

Required

true

Suppress Configuration Validator: JMS User

Description

Whether to suppress configuration warnings produced by the JMS User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_policies_jms_user

Required

true

Suppress Configuration Validator: SAML Entity Base URL

Description

Whether to suppress configuration warnings produced by the SAML Entity Base URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_entity_base_url

Required

true

Suppress Configuration Validator: SAML Entity ID

Description

Whether to suppress configuration warnings produced by the SAML Entity ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_entity_id

Required

true

Suppress Configuration Validator: Alias of SAML Sign/Encrypt Private Key

Description

Whether to suppress configuration warnings produced by the Alias of SAML Sign/Encrypt Private Key configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_key_alias

Required

true

Suppress Configuration Validator: SAML Sign/Encrypt Private Key Password

Description

Whether to suppress configuration warnings produced by the SAML Sign/Encrypt Private Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_key_password

Required

true

Suppress Configuration Validator: SAML Keystore Password

Description

Whether to suppress configuration warnings produced by the SAML Keystore Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_keystore_password

Required

true

Suppress Configuration Validator: Path to SAML Keystore File

Description

Whether to suppress configuration warnings produced by the Path to SAML Keystore File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_keystore_path

Required

true

Suppress Configuration Validator: SAML Login URL

Description

Whether to suppress configuration warnings produced by the SAML Login URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_login_url

Required

true

Suppress Configuration Validator: Path to SAML IDP Metadata File

Description

Whether to suppress configuration warnings produced by the Path to SAML IDP Metadata File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_metadata_path

Required

true

Suppress Configuration Validator: SAML Attribute Identifier for User Role

Description

Whether to suppress configuration warnings produced by the SAML Attribute Identifier for User Role configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_oid_role

Required

true

Suppress Configuration Validator: SAML Attribute Identifier for User ID

Description

Whether to suppress configuration warnings produced by the SAML Attribute Identifier for User ID configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_oid_user

Required

true

Suppress Configuration Validator: SAML Attribute Values for Roles

Description

Whether to suppress configuration warnings produced by the SAML Attribute Values for Roles configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_role_map

Required

true

Suppress Configuration Validator: Path to SAML Role Assignment Script

Description

Whether to suppress configuration warnings produced by the Path to SAML Role Assignment Script configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_saml_role_script

Required

true

Suppress Configuration Validator: Default Facets

Description

Whether to suppress configuration warnings produced by the Default Facets configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_search_default_facets

Required

true

Suppress Configuration Validator: Cloudera Telemetry Publisher S3 Bucket

Description

Whether to suppress configuration warnings produced by the Cloudera Telemetry Publisher S3 Bucket configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_nav_telemetry_bucket_name

Required

true

Suppress Configuration Validator: Audit Event Filter

Description

Whether to suppress configuration warnings produced by the Audit Event Filter configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_audit_event_filter

Required

true

Suppress Configuration Validator: Navigator Metadata Server Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Client Advanced Configuration Snippet (Safety Valve) for navigator.client.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_client_config_safety_valve

Required

true

Suppress Configuration Validator: Navigator Audit Server Database Hostname

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Database Hostname configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_host

Required

true

Suppress Configuration Validator: Navigator Audit Server Database Name

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Database Name configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_name

Required

true

Suppress Configuration Validator: Navigator Audit Server Database Password

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Database Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_password

Required

true

Suppress Configuration Validator: Navigator Audit Server Database Username

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Database Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_database_user

Required

true

Suppress Configuration Validator: Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for db.navigator.properties

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for db.navigator.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_db_safety_valve

Required

true

Suppress Configuration Validator: Navigator Audit Server Web UI Port

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Web UI Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_debug_port

Required

true

Suppress Configuration Validator: Java Configuration Options for Navigator Audit

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Navigator Audit configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_java_opts

Required

true

Suppress Configuration Validator: Kafka Topic

Description

Whether to suppress configuration warnings produced by the Kafka Topic configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_kafka_publishing_topic

Required

true

Suppress Configuration Validator: Navigator Audit Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_role_env_safety_valve

Required

true

Suppress Configuration Validator: Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_safety_valve

Required

true

Suppress Configuration Validator: Navigator Audit Server Port

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_server_port

Required

true

Suppress Configuration Validator: Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_server_safety_valve

Required

true

Suppress Configuration Validator: Navigator TLS/SSL Trust Store File

Description

Whether to suppress configuration warnings produced by the Navigator TLS/SSL Trust Store File configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_truststore_file

Required

true

Suppress Configuration Validator: Navigator TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the Navigator TLS/SSL Trust Store Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigator_truststore_password

Required

true

Suppress Configuration Validator: Navigator Metadata Server Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_navigatormetaserver_role_env_safety_valve

Required

true

Suppress Configuration Validator: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the Heap Dump Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Exporters Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Extensions Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Processors Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Receivers Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write URL configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Remote Write Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Configuration Validator: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the OpenTelemetry Collector Service Section configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Configuration Validator: PII Masking Regular Expression

Description

Whether to suppress configuration warnings produced by the PII Masking Regular Expression configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_pii_masking_regex

Required

true

Suppress Configuration Validator: Prometheus adapter configuration

Description

Whether to suppress configuration warnings produced by the Prometheus adapter configuration configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_adapter_config

Required

true

Suppress Configuration Validator: Prometheus Metrics Endpoint Password

Description

Whether to suppress configuration warnings produced by the Prometheus Metrics Endpoint Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_password

Required

true

Suppress Configuration Validator: Prometheus Metrics Endpoint Port

Description

Whether to suppress configuration warnings produced by the Prometheus Metrics Endpoint Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_port

Required

true

Suppress Configuration Validator: Prometheus Metrics Endpoint Username

Description

Whether to suppress configuration warnings produced by the Prometheus Metrics Endpoint Username configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_prometheus_metrics_endpoint_username

Required

true

Suppress Configuration Validator: Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.db.properties

Description

Whether to suppress configuration warnings produced by the Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.db.properties configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_db_safety_valve

Required

true

Suppress Configuration Validator: Reports Manager Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Reports Manager Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_role_env_safety_valve

Required

true

Suppress Configuration Validator: Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.conf

Description

Whether to suppress configuration warnings produced by the Reports Manager Advanced Configuration Snippet (Safety Valve) for headlamp.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_reportsmanager_safety_valve

Required

true

Suppress Configuration Validator: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the Custom Control Group Resources (overrides Cgroup settings) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Configuration Validator: Role Triggers

Description

Whether to suppress configuration warnings produced by the Role Triggers configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Configuration Validator: Service Monitor Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Service Monitor Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_servicemonitor_role_env_safety_valve

Required

true

Suppress Configuration Validator: SNMP Validator

Description

Whether to suppress configuration warnings produced by the SNMP Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_snmp_validator

Required

true

Suppress Configuration Validator: TLS/SSL Keystore Key Password

Description

Whether to suppress configuration warnings produced by the TLS/SSL Keystore Key Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Configuration Validator: Firehose Debug Server TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the Firehose Debug Server TLS/SSL Server Keystore File Location configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Configuration Validator: Firehose Debug Server TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the Firehose Debug Server TLS/SSL Server Keystore File Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Configuration Validator: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the Stacks Collection Directory configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Configuration Validator: Telemetry Publisher Web UI Port.

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Web UI Port. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_debug_port

Required

true

Suppress Configuration Validator: Telemetry Publisher Web UI IPaddress.

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Web UI IPaddress. configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_debug_server_interface

Required

true

Suppress Configuration Validator: Telemetry Publisher Server Port

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Server Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_server_port

Required

true

Suppress Configuration Validator: Java Configuration Options for Telemetry Publisher

Description

Whether to suppress configuration warnings produced by the Java Configuration Options for Telemetry Publisher configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_java_opts

Required

true

Suppress Configuration Validator: Proxy Password

Description

Whether to suppress configuration warnings produced by the Proxy Password configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_password

Required

true

Suppress Configuration Validator: Proxy Port

Description

Whether to suppress configuration warnings produced by the Proxy Port configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_port

Required

true

Suppress Configuration Validator: Proxy Server

Description

Whether to suppress configuration warnings produced by the Proxy Server configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_server

Required

true

Suppress Configuration Validator: Proxy User

Description

Whether to suppress configuration warnings produced by the Proxy User configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_user

Required

true

Suppress Configuration Validator: Telemetry Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Environment Advanced Configuration Snippet (Safety Valve) configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_role_env_safety_valve

Required

true

Suppress Configuration Validator: Telemetry Publisher Advanced Configuration Snippet (Safety Valve) for telemetrypublisher.conf

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Advanced Configuration Snippet (Safety Valve) for telemetrypublisher.conf configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_safety_valve

Required

true

Suppress Configuration Validator: Telemetry Kerberos Principal for HDFS

Description

Whether to suppress configuration warnings produced by the Telemetry Kerberos Principal for HDFS configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_tp_hdfs_kerberos_princ

Required

true

Suppress Configuration Validator: YARN MapReduce Counter Descriptions

Description

Whether to suppress configuration warnings produced by the YARN MapReduce Counter Descriptions configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_yarn_application_mapreduce_counters

Required

true

Suppress Configuration Validator: Activity Monitor - Unsupported Since 7.0.0 Count Validator

Description

Whether to suppress configuration warnings produced by the Activity Monitor - Unsupported Since 7.0.0 Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_activitymonitor_count_validator

Required

true

Suppress Configuration Validator: Alert Publisher Count Validator

Description

Whether to suppress configuration warnings produced by the Alert Publisher Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_alertpublisher_count_validator

Required

true

Suppress Configuration Validator: Event Server Count Validator

Description

Whether to suppress configuration warnings produced by the Event Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_eventserver_count_validator

Required

true

Suppress Configuration Validator: Host Monitor Count Validator

Description

Whether to suppress configuration warnings produced by the Host Monitor Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_hostmonitor_count_validator

Required

true

Suppress Configuration Validator: Cloudera Management Service Host Colocation Validator

Description

Whether to suppress configuration warnings produced by the Cloudera Management Service Host Colocation Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_mgmt_colocation_validator

Required

true

Suppress Parameter Validation: Cloudera Management Service Service Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Management Service Service Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_mgmt_service_env_safety_valve

Required

true

Suppress Parameter Validation: Cloudera Management Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Management Service Advanced Configuration Snippet (Safety Valve) for ssl-client.xml parameter.

Related Name

Default Value

false

API Name

service_config_suppression_mgmt_ssl_client_safety_valve

Required

true

Suppress Configuration Validator: Navigator Audit Server Count Validator

Description

Whether to suppress configuration warnings produced by the Navigator Audit Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_count_validator

Required

true

Suppress Parameter Validation: Small Files Reporting: HDFS Staging Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Small Files Reporting: HDFS Staging Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_navigator_smallfiles_hdfs_path

Required

true

Suppress Configuration Validator: Navigator Metadata Server Count Validator

Description

Whether to suppress configuration warnings produced by the Navigator Metadata Server Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_navigatormetaserver_count_validator

Required

true

Suppress Parameter Validation: System Group

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System Group parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_groupname

Required

true

Suppress Parameter Validation: System User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the System User parameter.

Related Name

Default Value

false

API Name

service_config_suppression_process_username

Required

true

Suppress Configuration Validator: Reports Manager Count Validator

Description

Whether to suppress configuration warnings produced by the Reports Manager Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_reportsmanager_count_validator

Required

true

Suppress Parameter Validation: Service Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Triggers parameter.

Related Name

Default Value

false

API Name

service_config_suppression_service_triggers

Required

true

Suppress Configuration Validator: Service Monitor Count Validator

Description

Whether to suppress configuration warnings produced by the Service Monitor Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_servicemonitor_count_validator

Required

true

Suppress Parameter Validation: Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Service Monitor Derived Configs Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

service_config_suppression_smon_derived_configs_safety_valve

Required

true

Suppress Parameter Validation: TLS/SSL Client Truststore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the TLS/SSL Client Truststore File Location parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_location

Required

true

Suppress Parameter Validation: Cloudera Manager Server TLS/SSL Trust Store Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Cloudera Manager Server TLS/SSL Trust Store Password parameter.

Related Name

Default Value

false

API Name

service_config_suppression_ssl_client_truststore_password

Required

true

Suppress Configuration Validator: Telemetry Publisher Count Validator

Description

Whether to suppress configuration warnings produced by the Telemetry Publisher Count Validator configuration validator.

Related Name

Default Value

false

API Name

service_config_suppression_telemetrypublisher_count_validator

Required

true

Suppress Health Test: KDC Server Connection Health

Description

Whether to suppress the results of the KDC Server Connection Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_kdc_availability

Required

true

Suppress Health Test: LDAP Server Connection Health

Description

Whether to suppress the results of the LDAP Server Connection Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_ldap_availability

Required

true

Suppress Health Test: Activity Monitor - Unsupported Since 7.0.0 Health

Description

Whether to suppress the results of the Activity Monitor - Unsupported Since 7.0.0 Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_activity_monitor_health

Required

true

Suppress Health Test: Alert Publisher Health

Description

Whether to suppress the results of the Alert Publisher Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_alert_publisher_health

Required

true

Suppress Health Test: Certificate Expiration

Description

Whether to suppress the results of the Certificate Expiration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_certificates_expiry

Required

true

Suppress Health Test: Cloudera Manager Server Clock Offset

Description

Whether to suppress the results of the Cloudera Manager Server Clock Offset heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_clock_offset_with_smon

Required

true

Suppress Health Test: Cloudera Manager Server Cluster Availability

Description

Whether to suppress the results of the Cloudera Manager Server Cluster Availability heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_cm_ha_availability

Required

true

Suppress Health Test: Command Storage Directory Free Space

Description

Whether to suppress the results of the Command Storage Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_command_storage_directory_free_space

Required

true

Suppress Health Test: Embedded Database Free Space

Description

Whether to suppress the results of the Embedded Database Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_embedded_db_free_space

Required

true

Suppress Health Test: Event Server Health

Description

Whether to suppress the results of the Event Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_event_server_health

Required

true

Suppress Health Test: Cloudera Manager Server Heap Size

Description

Whether to suppress the results of the Cloudera Manager Server Heap Size heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_heap_size

Required

true

Suppress Health Test: Host Monitor Health

Description

Whether to suppress the results of the Host Monitor Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_host_monitor_health

Required

true

Suppress Health Test: Navigator Audit Server Health

Description

Whether to suppress the results of the Navigator Audit Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_navigator_health

Required

true

Suppress Health Test: Navigator Metadata Server Health

Description

Whether to suppress the results of the Navigator Metadata Server Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_navigatormetaserver_health

Required

true

Suppress Health Test: Cloudera Manager Server Pause Duration

Description

Whether to suppress the results of the Cloudera Manager Server Pause Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_pause_duration

Required

true

Suppress Health Test: Reports Manager Health

Description

Whether to suppress the results of the Reports Manager Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_reports_manager_health

Required

true

Suppress Health Test: Service Monitor Health

Description

Whether to suppress the results of the Service Monitor Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_service_monitor_health

Required

true

Suppress Health Test: Telemetry Publisher Health

Description

Whether to suppress the results of the Telemetry Publisher Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

service_health_suppression_mgmt_telemetrypublisher_health

Required

true

Telemetry Publisher

Advanced

Telemetry Publisher Export Period

Description

The export period in seconds.

Related Name

export.period

Default Value

1 minute(s)

API Name

export_period

Required

true

Telemetry Publisher Logging Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, a string to be inserted into log4j.properties for this role only.

Related Name

Default Value

API Name

log4j_safety_valve

Required

false

Enable auto refresh for metric configurations

Description

When true, Enable Metric Collection and Metric Filter parameters will be set automatically if they're changed. Otherwise, a refresh by hand is required.

Related Name

Default Value

false

API Name

metric_config_auto_refresh

Required

false

Telemetry Publisher Data Directory

Description

Storage for tracking persistent state of the role.

Related Name

data.dir

Default Value

/var/lib/cloudera-scm-telemetrypublisher

API Name

mgmt_data_dir

Required

false

Heap Dump Directory

Description

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it does not exist. If this directory already exists, it will be owned by the current role user with 1777 permissions. Sharing the same directory among multiple roles will cause an ownership race. The heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

Related Name

oom_heap_dump_dir

Default Value

/tmp

API Name

oom_heap_dump_dir

Required

false

Dump Heap for Cloudera Management Service When Out of Memory

Description

When set, generates a heap dump file for Cloudera Management Service when an out-of-memory error occurs.

Related Name

Default Value

false

API Name

oom_heap_dump_enabled

Required

true

Kill When Out of Memory

Description

When set, a SIGKILL signal is sent to the role process when java.lang.OutOfMemoryError is thrown.

Related Name

Default Value

true

API Name

oom_sigkill_enabled

Required

true

Telemetry Publisher Polling Period

Description

The extractor polling period in seconds.

Related Name

extractor.poll_period

Default Value

1 minute(s)

API Name

poll_period

Required

true

Automatically Restart Process

Description

When set, this role's process is automatically (and transparently) restarted in the event of an unexpected failure. This configuration applies in the time after the Start Wait Timeout period.

Related Name

Default Value

true

API Name

process_auto_restart

Required

true

Enable Metric Collection

Description

Cloudera Manager agent monitors each service and each of its role by publishing metrics to the Cloudera Manager Service Monitor. Setting it to false will stop Cloudera Manager agent from publishing any metric for corresponding service/roles. This is usually helpful for services that generate large amount of metrics which Service Monitor is not able to process.

Related Name

Default Value

true

API Name

process_should_monitor

Required

true

Process Start Retry Attempts

Description

Number of times to try starting a role's process when the process exits before the Start Wait Timeout period. After a process is running beyond the Start Wait Timeout, the retry count is reset. Setting this configuration to zero will prevent restart of the process during the Start Wait Timeout period.

Related Name

Default Value

3

API Name

process_start_retries

Required

false

Process Start Wait Timeout

Description

The time in seconds to wait for a role's process to start successfully on a host. Processes which exit/crash before this time will be restarted until reaching the limit specified by the Start Retry Attempts count parameter. Setting this configuration to zero will turn off this feature.

Related Name

Default Value

20

API Name

process_start_secs

Required

false

Java Configuration Options for Telemetry Publisher

Description

These arguments will be passed as part of the Java command line. Commonly, garbage collection flags, PermGen, or extra debugging flags would be passed here. Note: When CM version is 6.3.0 or greater, {{JAVA_GC_ARGS}} will be replaced by JVM Garbage Collection arguments based on the runtime Java JVM version.

Related Name

Default Value

API Name

telemetrypublisher_java_opts

Required

false

Log and Query Redaction

Description

Telemetry Publisher recommends and by default requires that Log and Query Redaction be enabled for all CDH clusters. If disabled for any cluster, an alert will be raised during role start. Disable this setting to allow running without redaction.

Related Name

log_query_redaction

Default Value

true

API Name

telemetrypublisher_log_query_redaction

Required

true

Proxy Support for Telemetry Publisher

Description

When set, Telemetry Publisher sends telemetry through a proxy server.

Related Name

telemetrypublisher.proxy.enabled

Default Value

false

API Name

telemetrypublisher_proxy_enabled

Required

false

Proxy Password

Description

Proxy Server Password. This configuration is used only when proxy support is enabled for Telemetry Publisher.

Related Name

telemetrypublisher.proxy.password

Default Value

API Name

telemetrypublisher_proxy_password

Required

false

Proxy Port

Description

Proxy Server Port. This configuration is used only when proxy support is enabled for Telemetry Publisher.

Related Name

telemetrypublisher.proxy.port

Default Value

API Name

telemetrypublisher_proxy_port

Required

false

Proxy Server

Description

Proxy Server Hostname. This configuration is used only when proxy support is enabled for Telemetry Publisher.

Related Name

telemetrypublisher.proxy.server

Default Value

API Name

telemetrypublisher_proxy_server

Required

false

Proxy User

Description

Proxy Server User. This configuration is used only when proxy support is enabled for Telemetry Publisher.

Related Name

telemetrypublisher.proxy.user

Default Value

API Name

telemetrypublisher_proxy_user

Required

false

Telemetry Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

For advanced use only, key-value pairs (one on each line) to be inserted into a role's environment. Applies to configurations of this role except client configuration.

Related Name

Default Value

API Name

TELEMETRYPUBLISHER_role_env_safety_valve

Required

false

Telemetry Publisher Advanced Configuration Snippet (Safety Valve) for telemetrypublisher.conf

Description

For advanced use only. A string to be inserted into telemetrypublisher.conf for this role only.

Related Name

Default Value

API Name

telemetrypublisher_safety_valve

Required

false

Telemetry Publisher Thread Pool Size

Description

The number of parallel threads used for extractor task execution.

Related Name

extractor.thread_pool_size

Default Value

10

API Name

thread_pool_size

Required

true

Logs

Telemetry Publisher Logging Threshold

Description

The minimum log level for Telemetry Publisher logs

Related Name

Default Value

INFO

API Name

log_threshold

Required

false

Telemetry Publisher Maximum Log File Backups

Description

The maximum number of rolled log files to keep for Telemetry Publisher logs. Typically used by log4j or logback.

Related Name

Default Value

10

API Name

max_log_backup_index

Required

false

Telemetry Publisher Max Log Size

Description

The maximum size, in megabytes, per log file for Telemetry Publisher logs. Typically used by log4j or logback.

Related Name

Default Value

200 MiB

API Name

max_log_size

Required

false

Telemetry Publisher Log Directory

Description

Directory where Telemetry Publisher will place its log files.

Related Name

Default Value

/var/log/cloudera-scm-telemetrypublisher

API Name

mgmt_log_dir

Required

false

Monitoring

Enable Health Alerts for this Role

Description

When set, Cloudera Manager will send alerts when the health of this role reaches the threshold specified by the EventServer setting eventserver_health_events_alert_threshold

Related Name

Default Value

true

API Name

enable_alerts

Required

false

Enable Configuration Change Alerts

Description

When set, Cloudera Manager will send alerts when this entity's configuration changes.

Related Name

Default Value

false

API Name

enable_config_alerts

Required

false

Heap Dump Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

heap_dump_directory_free_space_absolute_thresholds

Required

false

Heap Dump Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's heap dump directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Heap Dump Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

heap_dump_directory_free_space_percentage_thresholds

Required

false

Enable JMX Exporter (beta)

Description

JMX Exporter support is a beta feature. If enabled, CM configures the role to run JMX Exporter in agent mode with the provided port and YAML configuration. This exporter then can be used with the OpenTelemetry Collector feature. See the JMX Exporter documentation.

Related Name

Default Value

false

API Name

jmx_exporter_enabled

Required

true

JMX Exporter Port

Description

JMX Exporter needs a port to implement a Prometheus exporter.

Related Name

Default Value

API Name

jmx_exporter_port

Required

false

JMX Exporter configuration YAML

Description

This configuration is passed to JMX Exporter as it is. See the JMX Exporter documentation.

Related Name

Default Value

API Name

jmx_exporter_yaml

Required

false

Log Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

log_directory_free_space_absolute_thresholds

Required

false

Log Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's log directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Log Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

log_directory_free_space_percentage_thresholds

Required

false

Rules to Extract Events from Log Files

Description

This file contains the rules that govern how log messages are turned into events by the custom log4j appender that this role loads. It is in JSON format, and is composed of a list of rules. Every log message is evaluated against each of these rules in turn to decide whether or not to send an event for

that message. If a log message matches multiple rules, the first matching rule is used.. Each rule has some or all of the following fields:

- alert - whether or not events generated from this rule should be promoted to alerts. A value of "true" will cause alerts to be generated. If not specified, the default is "false".
- rate (mandatory) - the maximum number of log messages matching this rule that can be sent as events every minute. If more than rate matching log messages are received in a single minute, the extra messages are ignored. If rate is less than 0, the number of messages per minute is unlimited.
- periodminutes - the number of minutes during which the publisher will only publish rate events or fewer. If not specified, the default is one minute
- threshold - apply this rule only to messages with this log4j severity level or above. An example is "WARN" for warning level messages or higher.
- content - match only those messages for which contents match this regular expression.
- exceptiontype - match only those messages that are part of an exception message. The exception type must match this regular expression.

Example:

- {"alert": false, "rate": 10, "exceptiontype": "java.lang.StringIndexOutOfBoundsException"}This rule sends events to Cloudera Manager for every StringIndexOutOfBoundsException, up to a maximum of 10 every minute.
- {"alert": false, "rate": 1, "periodminutes": 1, "exceptiontype": ".*"}, {"alert": true, "rate": 1, "periodminutes": 1, "threshold":"ERROR"}In this example, an event generated may not be promoted to alert if an exception is in the ERROR log message, because the first rule with alert = false will match.

Related Name

Default Value

version: 0, rules: [alert: false, rate: 1, periodminutes: 1, threshold: FATAL , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Instead, use .* , alert: false, rate: 0, threshold: WARN, content: .* is deprecated. Use .* instead , alert: false, rate: 0, threshold: ALL, content: .*AUTOACTIONTRIGGER.* , alert: false, rate: 1, periodminutes: 2, exceptiontype: .* , alert: false, rate: 1, periodminutes: 1, threshold: WARN]

API Name

log_event_whitelist

Required

false

Metric Filter

Description

Defines a Metric Filter for this role. Cloudera Manager Agents will not send filtered metrics to the Service Monitor. Define the following fields:

- Health Test Metric Set - Select this parameter to collect only metrics required for health tests.
- Default Dashboard Metric Set - Select this parameter to collect only metrics required for the default dashboards. For user-defined charts, you must add the metrics you require for the chart using the Custom Metrics parameter.
- Include/Exclude Custom Metrics - Select Include to specify metrics that should be collected. Select Exclude to specify metrics that should not be collected. Enter the metric names to be included or excluded using the Metric Name parameter.
- Metric Name - The name of a metric that will be included or excluded during metric collection.

If you do not select Health Test Metric Set or Default Dashboard Metric Set, or specify metrics by name, metric filtering will be turned off (this is the default behavior).For example, the following

configuration enables the collection of metrics required for Health Tests and the jvm_heap_used_mb metric:

- Include only Health Test Metric Set: Selected.
- Include/Exclude Custom Metrics: Set to Include.
- Metric Name: jvm_heap_used_mb

You can also view the JSON representation for this parameter by clicking View as JSON. In this example, the JSON looks like this:{ "includeHealthTestMetricSet": true, "filterType": "whitelist", "metrics": ["jvm_heap_used_mb"] }

Related Name

Default Value

API Name

monitoring_metric_filter

Required

false

OpenTelemetry Collector Exporters Section

Description

Define the exporters settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

exporters: prometheusremotewrite/$ROLE_NAME: endpoint: $ROLE_PARAM(otelcol_remote_write_url) auth: authenticator: basicauth/common tls: insecure_skip_verify: true retry_on_failure: enabled: true initial_interval: 10s max_interval: 40s max_elapsed_time: 300s

API Name

otelcol_exporters

Required

false

OpenTelemetry Collector Extensions Section

Description

Define the extensions settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

extensions: basicauth/common: client_auth: username: $ROLE_PARAM(otelcol_remote_write_user) password: '$ROLE_PARAM(otelcol_remote_write_password)'

API Name

otelcol_extensions

Required

false

OpenTelemetry Collector Processors Section

Description

Define the processors settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_processors

Required

false

OpenTelemetry Collector Receivers Section

Description

Define the receivers settings as a yaml snippet according to the OpenTelemetry Collector standards. A number of variables can help to use the same config everywhere. The follow strings or expressions will be substituted: $HOST_NAME, $CLUSTER_NAME, $CLUSTER_ID, $SERVICE_TYPE, $SERVICE_NAME, $ROLE_NAME, $ROLE_TYPE, $ROLE_PARAM(my_parameter_name) - e.g.: a port parameter for the role's metrics, $DECODE_B64(...) and $DECODE_URL(...) to decode encoded parameters, $ENV_PARAM(name) to fetch params from the process' environment, $SYS_PARAM(name) to fetch java system properties.

Related Name

Default Value

API Name

otelcol_receivers

Required

false

OpenTelemetry Collector Remote Write Password

Description

Remote write password for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_password) expression. Specify $INFRA(cdp_request_signer_password) when forwarding to Cloudera Observability central monitoring. (This is the default.)

Related Name

Default Value

******

API Name

otelcol_remote_write_password

Required

false

OpenTelemetry Collector Remote Write URL

Description

Remote write URL for the OpenTelemetry Collector. This param is for convenience and intended to be used at the exporters section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_url) expression. Specify $INFRA(cdp_request_signer_url) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_url)

API Name

otelcol_remote_write_url

Required

false

OpenTelemetry Collector Remote Write Username

Description

Remote write username for the OpenTelemetry Collector. This param is for convenience and intended to be used at the extensions section of Otelcol settings using the $ROLE_PARAM(otelcol_remote_write_user) expression. Specify $INFRA(cdp_request_signer_username) when forwarding to Cloudera Observability central monitoring.

Related Name

Default Value

$INFRA(cdp_request_signer_username)

API Name

otelcol_remote_write_user

Required

false

OpenTelemetry Collector Service Section

Description

Define the service settings as a yaml snippet according to the OpenTelemetry Collector standards. Variable substitution available, see the receivers' help.

Related Name

Default Value

API Name

otelcol_service

Required

false

Enable OpenTelemetry Collector (beta)

Description

OpenTelemetry Collector support is a new beta feature (will change without notice) which can run OpenTelemetry Collector as an agent together with the CM Agent to forward metrics to a Prometheus like storage.

Related Name

Default Value

false

API Name

otelcol_should_collect

Required

true

Swap Memory Usage Rate Thresholds

Description

The health test thresholds on the swap memory usage rate of the process. Specified as the change of the used swap memory during the predefined period.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

process_swap_memory_rate_thresholds

Required

false

Swap Memory Usage Rate Window

Description

The period to review when computing unexpected swap memory usage change of the process.

Related Name

common.process.swap_memory_rate_window

Default Value

5 minute(s)

API Name

process_swap_memory_rate_window

Required

false

Process Swap Memory Thresholds

Description

The health test thresholds on the swap memory usage of the process. This takes precedence over the host level threshold.

Related Name

Default Value

Warning: 200 B, Critical: Never

API Name

process_swap_memory_thresholds

Required

false

Role Triggers

Description

The configured triggers for this role. This is a JSON-formatted list of triggers. These triggers are evaluated as part as the health system. Every trigger expression is parsed, and if the trigger condition is met, the list of actions provided in the trigger expression is executed. Each trigger has the following fields:

- triggerName (mandatory) - The name of the trigger. This value must be unique for the specific role.

- triggerExpression (mandatory) - A tsquery expression representing the trigger.
- streamThreshold (optional) - The maximum number of streams that can satisfy a condition of a trigger before the condition fires. By default set to 0, and any stream returned causes the condition to fire.
- enabled (optional) - By default set to 'true'. If set to 'false', the trigger is not evaluated.
- expressionEditorConfig (optional) - Metadata for the trigger editor. If present, the trigger should only be edited from the Edit Trigger page; editing the trigger here can lead to inconsistencies.

For example, the following JSON formatted trigger configured for a DataNode fires if the DataNode has more than 1500 file descriptors opened:[{"triggerName": "sample-trigger", "triggerExpression": "IF (SELECT fd_open WHERE roleName=$ROLENAME and last(fd_open) > 1500) DO health:bad", "streamThreshold": 0, "enabled": "true"}]See the trigger rules documentation for more details on how to write triggers using tsquery.The JSON format is evolving and may change and, as a result, backward compatibility is not guaranteed between releases.

Related Name

Default Value

[]

API Name

role_triggers

Required

true

Telemetry Publisher Data Directory Free Space Monitoring Absolute Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Telemetry Publisher Data Directory.

Related Name

Default Value

Warning: 10 GiB, Critical: 5 GiB

API Name

telemetrypublisher_data_directory_free_space_absolute_thresholds

Required

false

Telemetry Publisher Data Directory Free Space Monitoring Percentage Thresholds

Description

The health test thresholds for monitoring of free space on the filesystem that contains this role's Telemetry Publisher Data Directory. Specified as a percentage of the capacity on that filesystem. This setting is not used if a Telemetry Publisher Data Directory Free Space Monitoring Absolute Thresholds setting is configured.

Related Name

Default Value

Warning: Never, Critical: Never

API Name

telemetrypublisher_data_directory_free_space_percentage_thresholds

Required

false

Metrics Data Export Failure Thresholds

Description

The health test thresholds for monitoring the data export failure count.

Related Name

Default Value

Warning: 3.0 time(s), Critical: 5.0 time(s)

API Name

telemetrypublisher_data_export_failure_thresholds

Required

true

Telemetry Publisher Data Export Monitoring Time Period

Description

The time period over which the telemetry publisher data export for streams will be monitored for failed export.

Related Name

Default Value

5 minute(s)

API Name

telemetrypublisher_data_export_failure_window

Required

true

Metrics Data Ingest Failure Thresholds

Description

The health test thresholds for monitoring the data ingest failure count.

Related Name

Default Value

Warning: 3.0 time(s), Critical: 5.0 time(s)

API Name

telemetrypublisher_data_ingest_failure_thresholds

Required

true

Telemetry Publisher Data Ingest Monitoring Time Period

Description

The time period over which the telemetry publisher data ingest for streams will be monitored for failed injest.

Related Name

Default Value

5 minute(s)

API Name

telemetrypublisher_data_ingest_failure_window

Required

true

File Descriptor Monitoring Thresholds

Description

The health test thresholds of the number of file descriptors used. Specified as a percentage of file descriptor limit.

Related Name

Default Value

Warning: 50.0 %, Critical: 70.0 %

API Name

telemetrypublisher_fd_thresholds

Required

false

Garbage Collection Duration Thresholds

Description

The health test thresholds for the weighted average time spent in Java garbage collection. Specified as a percentage of elapsed wall clock time.

Related Name

Default Value

Warning: 30.0, Critical: 60.0

API Name

telemetrypublisher_gc_duration_thresholds

Required

false

Garbage Collection Duration Monitoring Period

Description

The period to review when computing the moving average of garbage collection time.

Related Name

Default Value

5 minute(s)

API Name

telemetrypublisher_gc_duration_window

Required

false

Telemetry Publisher Host Health Test

Description

When computing the overall Telemetry Publisher health, consider the host's health.

Related Name

Default Value

true

API Name

telemetrypublisher_host_health_enabled

Required

false

Telemetry Publisher Process Health Test

Description

Enables the health test that the Telemetry Publisher's process state is consistent with the role configuration

Related Name

Default Value

true

API Name

telemetrypublisher_scm_health_enabled

Required

false

Web Metric Collection

Description

Enables the health test that the Cloudera Manager Agent can successfully contact and gather metrics from the web server.

Related Name

Default Value

true

API Name

telemetrypublisher_web_metric_collection_enabled

Required

false

Web Metric Collection Duration

Description

The health test thresholds on the duration of the metrics request to the web server.

Related Name

Default Value

Warning: 10 second(s), Critical: Never

API Name

telemetrypublisher_web_metric_collection_thresholds

Required

false

Unexpected Exits Thresholds

Description

The health test thresholds for unexpected exits encountered within a recent period specified by the unexpected_exits_window configuration for the role.

Related Name

Default Value

Warning: Never, Critical: Any

API Name

unexpected_exits_thresholds

Required

false

Unexpected Exits Monitoring Period

Description

The period to review when computing unexpected exits.

Related Name

Default Value

5 minute(s)

API Name

unexpected_exits_window

Required

false

Other

Telemetry Publisher Web UI IPaddress.

Description

The IP where Telemetry Publisher starts a debug web server.

Related Name

telemetry_publisher.debug.server.interface

Default Value

0.0.0.0

API Name

telemetry_publisher_debug_server_interface

Required

false

Performance

Maximum Process File Descriptors

Description

If configured, overrides the process soft and hard rlimits (also called ulimits) for file descriptors to the configured value.

Related Name

Default Value

API Name

rlimit_fds

Required

false

Ports and Addresses

Telemetry Publisher Web UI Port.

Description

The port where Telemetry Publisher starts a debug web server. Set to -1 to disable debug server.

Related Name

telemetry_publisher.debug.port

Default Value

10111

API Name

telemetry_publisher_debug_port

Required

false

Telemetry Publisher Server Port

Description

The port where Telemetry Publisher listens for requests

Related Name

telemetry_publisher.server.port

Default Value

10110

API Name

telemetry_publisher_server_port

Required

false

Resource Management

Cgroup CPU Shares

Description

Number of CPU shares to assign to this role. The greater the number of shares, the larger the share of the host's CPUs that will be given to this role when the host experiences CPU contention. Must be between 2 and 262144. Defaults to 1024 for processes not managed by Cloudera Manager.

Related Name

cpu.shares

Default Value

1024

API Name

rm_cpu_shares

Required

true

Custom Control Group Resources (overrides Cgroup settings)

Description

Custom control group resources to assign to this role, which will be enforced by the Linux kernel. These resources should exist on the target hosts, otherwise an error will occur when the process starts. Use the same format as used for arguments to the cgexec command: resource1,resource2:path1 or resource3:path2 For example: 'cpu,memory:my/path blkio:my2/path2' ***These settings override other cgroup settings.***

Related Name

custom.cgroups

Default Value

API Name

rm_custom_resources

Required

false

Cgroup I/O Weight

Description

Weight for the read I/O requests issued by this role. The greater the weight, the higher the priority of the requests when the host experiences I/O contention. Must be between 100 and 1000. Defaults to 1000 for processes not managed by Cloudera Manager.

Related Name

blkio.weight

Default Value

500

API Name

rm_io_weight

Required

true

Cgroup Memory Hard Limit

Description

Hard memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_hard_limit

Required

true

Cgroup Memory Soft Limit

Description

Soft memory limit to assign to this role, enforced by the Linux kernel. When the limit is reached, the kernel will reclaim pages charged to the process if and only if the host is facing memory pressure. If reclaiming fails, the kernel may kill the process. Both anonymous as well as page cache pages contribute to the limit. Use a value of -1 to specify no limit. By default processes not managed by Cloudera Manager will have no limit. If the value is -1, Cloudera Manager will not monitor Cgroup memory usage therefore some of the charts will show 'No Data'

Related Name

memory.soft_limit_in_bytes

Default Value

-1 MiB

API Name

rm_memory_soft_limit

Required

true

Java Heap Size of TelemetryPublisher in Bytes

Description

Maximum size in bytes for the Java Process heap memory. Passed to Java -Xmx.

Related Name

Default Value

1 GiB

API Name

telemetry_publisher_heapsize

Required

false

Security

Telemetry Kerberos Principal

Description

Kerberos principal used by Telemetry Publisher to authenticate to all services except HDFS. Note: Telemetry should use the principal used by Hue service if you are using MapReduce1 service in any of the clusters.

Related Name

Default Value

hue

API Name

kerberos_role_princ_name

Required

true

Enable TLS/SSL for Telemetry Publisher

Description

Encrypt communication between clients and Telemetry Publisher using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).

Related Name

telemetrypublisher.http.enable_ssl

Default Value

false

API Name

ssl_enabled

Required

false

Telemetry Publisher TLS/SSL Server Keystore Key Password

Description

The password that protects the private key contained in the keystore used when Telemetry Publisher is acting as a TLS/SSL server.

Related Name

telemetrypublisher.ssl.keyManagerPassword

Default Value

API Name

ssl_server_keystore_keypassword

Required

false

Telemetry Publisher TLS/SSL Server Keystore File Location

Description

The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Telemetry Publisher is acting as a TLS/SSL server. The keystore must be in the format specified in Administration > Settings > Java Keystore Type.

Related Name

telemetrypublisher.ssl.keyStorePath

Default Value

API Name

ssl_server_keystore_location

Required

false

Telemetry Publisher TLS/SSL Server Keystore File Password

Description

The password for the Telemetry Publisher keystore file.

Related Name

telemetrypublisher.ssl.keyStorePassword

Default Value

API Name

ssl_server_keystore_password

Required

false

Telemetry Kerberos Principal for HDFS

Description

Kerberos principal used by Telemetry Publisher to authenticate to HDFS services. Note: This principal must be in the same groups as the principals used by Job History and Spark History Servers.

Related Name

telemetrypublisher.dfs.user

Default Value

hdfs

API Name

tp_hdfs_kerberos_princ

Required

true

Stacks Collection

Stacks Collection Data Retention

Description

The amount of stacks data that is retained. After the retention limit is reached, the oldest data is deleted.

Related Name

stacks_collection_data_retention

Default Value

100 MiB

API Name

stacks_collection_data_retention

Required

false

Stacks Collection Directory

Description

The directory in which stacks logs are placed. If not set, stacks are logged into a stacks subdirectory of the role's log directory. If this directory already exists, it will be owned by the current role user with 755 permissions. Sharing the same directory among multiple roles will cause an ownership race.

Related Name

stacks_collection_directory

Default Value

API Name

stacks_collection_directory

Required

false

Stacks Collection Enabled

Description

Whether or not periodic stacks collection is enabled.

Related Name

stacks_collection_enabled

Default Value

false

API Name

stacks_collection_enabled

Required

true

Stacks Collection Frequency

Description

The frequency with which stacks are collected.

Related Name

stacks_collection_frequency

Default Value

5.0 second(s)

API Name

stacks_collection_frequency

Required

false

Stacks Collection Method

Description

The method used to collect stacks. The jstack option involves periodically running the jstack command against the role's daemon process. The servlet method is available for those roles that have an HTTP server endpoint exposing the current stacks traces of all threads. When the servlet method is selected, that HTTP endpoint is periodically scraped.

Related Name

stacks_collection_method

Default Value

jstack

API Name

stacks_collection_method

Required

false

Suppressions

Suppress Configuration Validator: CDH Version Validator

Description

Whether to suppress configuration warnings produced by the CDH Version Validator configuration validator.

Related Name

Default Value

false

API Name

role_config_suppression_cdh_version_validator

Required

true

Suppress Parameter Validation: JMX Exporter Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_port

Required

true

Suppress Parameter Validation: JMX Exporter configuration YAML

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the JMX Exporter configuration YAML parameter.

Related Name

Default Value

false

API Name

role_config_suppression_jmx_exporter_yaml

Required

true

Suppress Parameter Validation: Telemetry Kerberos Principal

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Kerberos Principal parameter.

Related Name

Default Value

false

API Name

role_config_suppression_kerberos_role_princ_name

Required

true

Suppress Parameter Validation: Telemetry Publisher Logging Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Logging Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log4j_safety_valve

Required

true

Suppress Parameter Validation: Rules to Extract Events from Log Files

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Rules to Extract Events from Log Files parameter.

Related Name

Default Value

false

API Name

role_config_suppression_log_event_whitelist

Required

true

Suppress Parameter Validation: Telemetry Publisher Data Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Data Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_data_dir

Required

true

Suppress Parameter Validation: Telemetry Publisher Log Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Log Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_mgmt_log_dir

Required

true

Suppress Parameter Validation: Heap Dump Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Heap Dump Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_oom_heap_dump_dir

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Exporters Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Exporters Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_exporters

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Extensions Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Extensions Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_extensions

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Processors Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Processors Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_processors

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Receivers Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Receivers Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_receivers

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_password

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write URL

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write URL parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_url

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Remote Write Username

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Remote Write Username parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_remote_write_user

Required

true

Suppress Parameter Validation: OpenTelemetry Collector Service Section

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the OpenTelemetry Collector Service Section parameter.

Related Name

Default Value

false

API Name

role_config_suppression_otelcol_service

Required

true

Suppress Parameter Validation: Custom Control Group Resources (overrides Cgroup settings)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Custom Control Group Resources (overrides Cgroup settings) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_rm_custom_resources

Required

true

Suppress Parameter Validation: Role Triggers

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Role Triggers parameter.

Related Name

Default Value

false

API Name

role_config_suppression_role_triggers

Required

true

Suppress Parameter Validation: Telemetry Publisher TLS/SSL Server Keystore Key Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher TLS/SSL Server Keystore Key Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_keypassword

Required

true

Suppress Parameter Validation: Telemetry Publisher TLS/SSL Server Keystore File Location

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher TLS/SSL Server Keystore File Location parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_location

Required

true

Suppress Parameter Validation: Telemetry Publisher TLS/SSL Server Keystore File Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher TLS/SSL Server Keystore File Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_ssl_server_keystore_password

Required

true

Suppress Parameter Validation: Stacks Collection Directory

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Stacks Collection Directory parameter.

Related Name

Default Value

false

API Name

role_config_suppression_stacks_collection_directory

Required

true

Suppress Parameter Validation: Telemetry Publisher Web UI Port.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Web UI Port. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_debug_port

Required

true

Suppress Parameter Validation: Telemetry Publisher Web UI IPaddress.

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Web UI IPaddress. parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_debug_server_interface

Required

true

Suppress Parameter Validation: Telemetry Publisher Server Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Server Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetry_publisher_server_port

Required

true

Suppress Parameter Validation: Java Configuration Options for Telemetry Publisher

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Java Configuration Options for Telemetry Publisher parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_java_opts

Required

true

Suppress Parameter Validation: Proxy Password

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Password parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_password

Required

true

Suppress Parameter Validation: Proxy Port

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Port parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_port

Required

true

Suppress Parameter Validation: Proxy Server

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy Server parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_server

Required

true

Suppress Parameter Validation: Proxy User

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Proxy User parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_proxy_user

Required

true

Suppress Parameter Validation: Telemetry Publisher Environment Advanced Configuration Snippet (Safety Valve)

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Environment Advanced Configuration Snippet (Safety Valve) parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_role_env_safety_valve

Required

true

Suppress Parameter Validation: Telemetry Publisher Advanced Configuration Snippet (Safety Valve) for telemetrypublisher.conf

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Publisher Advanced Configuration Snippet (Safety Valve) for telemetrypublisher.conf parameter.

Related Name

Default Value

false

API Name

role_config_suppression_telemetrypublisher_safety_valve

Required

true

Suppress Parameter Validation: Telemetry Kerberos Principal for HDFS

Description

Whether to suppress configuration warnings produced by the built-in parameter validation for the Telemetry Kerberos Principal for HDFS parameter.

Related Name

Default Value

false

API Name

role_config_suppression_tp_hdfs_kerberos_princ

Required

true

Suppress Health Test: Data Export Test For Stream Hive-App

Description

Whether to suppress the results of the Data Export Test For Stream Hive-App heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__app_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Hive-App

Description

Whether to suppress the results of the Data Ingest Test For Stream Hive-App heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__app_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Hive-Query-Audits

Description

Whether to suppress the results of the Data Export Test For Stream Hive-Query-Audits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__query__audits_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Hive-Query-Audits

Description

Whether to suppress the results of the Data Ingest Test For Stream Hive-Query-Audits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__query__audits_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Hive-Tez-App

Description

Whether to suppress the results of the Data Export Test For Stream Hive-Tez-App heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__tez__app_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Hive-Tez-App

Description

Whether to suppress the results of the Data Ingest Test For Stream Hive-Tez-App heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_hive__tez__app_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Impala-Query-Profile

Description

Whether to suppress the results of the Data Export Test For Stream Impala-Query-Profile heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impala__query__profile_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Impala-Query-Profile

Description

Whether to suppress the results of the Data Ingest Test For Stream Impala-Query-Profile heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_impala__query__profile_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Oozie-Workflows

Description

Whether to suppress the results of the Data Export Test For Stream Oozie-Workflows heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie__workflows_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Oozie-Workflows

Description

Whether to suppress the results of the Data Ingest Test For Stream Oozie-Workflows heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_oozie__workflows_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Spark2_on_yarn-Event-Log

Description

Whether to suppress the results of the Data Export Test For Stream Spark2_on_yarn-Event-Log heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark2_on_yarn__event__log_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Spark2_on_yarn-Event-Log

Description

Whether to suppress the results of the Data Ingest Test For Stream Spark2_on_yarn-Event-Log heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_spark2_on_yarn__event__log_data_ingest_failure

Required

true

Suppress Health Test: Audit Pipeline Test

Description

Whether to suppress the results of the Audit Pipeline Test heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_audit_health

Required

true

Suppress Health Test: Telemetry Publisher Data Directory Free Space

Description

Whether to suppress the results of the Telemetry Publisher Data Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_data_directory_free_space

Required

true

Suppress Health Test: File Descriptors

Description

Whether to suppress the results of the File Descriptors heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_file_descriptor

Required

true

Suppress Health Test: GC Duration

Description

Whether to suppress the results of the GC Duration heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_gc_duration

Required

true

Suppress Health Test: Heap Dump Directory Free Space

Description

Whether to suppress the results of the Heap Dump Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_heap_dump_directory_free_space

Required

true

Suppress Health Test: Host Health

Description

Whether to suppress the results of the Host Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_host_health

Required

true

Suppress Health Test: Log Directory Free Space

Description

Whether to suppress the results of the Log Directory Free Space heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_log_directory_free_space

Required

true

Suppress Health Test: Otelcol Health

Description

Whether to suppress the results of the Otelcol Health heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_otelcol_health

Required

true

Suppress Health Test: Process Status

Description

Whether to suppress the results of the Process Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_scm_health

Required

true

Suppress Health Test: Swap Memory Usage

Description

Whether to suppress the results of the Swap Memory Usage heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_swap_memory_usage

Required

true

Suppress Health Test: Swap Memory Usage Rate Beta

Description

Whether to suppress the results of the Swap Memory Usage Rate Beta heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_swap_memory_usage_rate

Required

true

Suppress Health Test: Unexpected Exits

Description

Whether to suppress the results of the Unexpected Exits heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_unexpected_exits

Required

true

Suppress Health Test: Web Server Status

Description

Whether to suppress the results of the Web Server Status heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_telemetrypublisher_web_metric_collection

Required

true

Suppress Health Test: Data Export Test For Stream Yarn-Apps

Description

Whether to suppress the results of the Data Export Test For Stream Yarn-Apps heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_yarn__apps_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Yarn-Apps

Description

Whether to suppress the results of the Data Ingest Test For Stream Yarn-Apps heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_yarn__apps_data_ingest_failure

Required

true

Suppress Health Test: Data Export Test For Stream Yarn-Jhist

Description

Whether to suppress the results of the Data Export Test For Stream Yarn-Jhist heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_yarn__jhist_data_export_failure

Required

true

Suppress Health Test: Data Ingest Test For Stream Yarn-Jhist

Description

Whether to suppress the results of the Data Ingest Test For Stream Yarn-Jhist heath test. The results of suppressed health tests are ignored when computing the overall health of the associated host, role or service, so suppressed health tests will not generate alerts.

Related Name

Default Value

false

API Name

role_health_suppression_yarn__jhist_data_ingest_failure

Required

true