Cloudera Manager 7.2.2

Release Notes

Date published: 2020-08-10
Date modified: 2020-09-17

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.2.2 Release Notes

Known Issues, Fixed Issues and New features for Cloudera Manager and CDP Private Cloud Base.

What's New in Cloudera Manager 7.2.2

New features and changed behavior for Cloudera Manager.

Alerts for Data Hub clusters can now be managed using Cloudera Manager.

Users with the EnvironmentAdmin Resource role are assigned to the Limited Cluster Administrator role in Cloudera Manager, which now allows you to manage alerts.

The Cloudera Management Service for Data Hub clusters can now be managed using Cloudera Manager.

Users with the EnvironmentAdmin Resource role are assigned to the Limited Cluster Administrator role in Cloudera Manager, which now allows you to configure, start, and stop the Cloudera Management Service.

Changes to how Cluster Templates handle null values

In Cloudera Manager, the cluster template contains key & value pairs of variables. However, keys without any value(s), get exported into the cluster template's json file. This can happen even if the Cloudera Manager Admin Console exposes the issue by showing up configuration warnings. Importing such templates to new clusters also introduces these warnings. Therefore, an export of such templates now requires the user to replace the 'null' value. Importing the template with such a key will fail with an error message.

Executing Impala queries monitoring related performance problems fixed. Memory usage is lowered.

Executing query monitoring is 100 times faster and memory consumption of this functionality is reduced 100 times .

Fixed Issues in Cloudera Manager 7.2.2

This topic lists the issues that have been fixed in Cloudera Manager since the previous release of Cloudera Manager.

Cloudera Bug: OPSAPS-57674: Knox should replace the resourceManager property (in scope of Oozie) using a new service instead of using JobTrackerServiceModelGenerator

By default, Cloudera Manager enables the new Resource Manager API service in the cdp-proxy-api topology in Knox, which is used for replacing the "resourceManager" property with the actual resource manager rpc:// address when an Oozie Job is submitted.

Cloudera Bug: OPSAPS-57429: Zookeeper SSL/TLS support for Oozie (CM change)

When SSL is enabled in Zookeeper, Oozie will try to connect to Zookeeper using SSL instead of a non-secure connection.

Cloudera Bug: OPSAPS-56678: SRM client configuration (srm.properties) contains invalid properties

New configuration resolvers have been added: file, system environment with default. This change is backward-compatible, and the old configuration works as usual.

Cloudera Bug: OPSAPS-57610: Schema Registry fails to come up on Ubuntu18 configs

When setting up the service the install script failed to properly set the "hdfs.kerberos.principal:" property.

Cloudera Bug: OPSAPS-54386: Upgrade swaggerui due to CVE

In version 42 of the Swagger-based Cloudera Manager API client, the types of some API model object fields have changed as compared to previous versions. In the Python client, several fields

have been migrated from type float to type int, and in the Java client several fields have been migrated from type BigDecimal to type Integer.

Cloudera Bug: OPSAPS-57158: CM API for Ozone credentials and rest info

A new endpoint has been added at /getOzoneS3Credentials under ClustersResource. This endpoint creates an Ozone S3 bucket with a specified name, and then returns Ozone AWS credentials. This affects versions CM/CDH>=7.1.3, CM/CDH>=7.2.2.

Cloudera Bug: OPSAPS-57802: Create 'MGMT' configuration authority, add it to global LCA role

Users with the global Limited Cluster Administrator role will now be able to update the Cloudera Management Service configuration, as well as perform power operations (start, stop, restart) on the Cloudera Management Service and its roles. This affects versions CM >= 7.2.2.

Cloudera Bug: OPSAPS-57467: Hardcoded parcel directory causes failure when non-standard path is used and TLS is enabled

The hardcoded parcel directory path from Schema Registry CSD is eliminated.

Cloudera Bug: OPSAPS-57411: Config for metrics fetching in group or separately

A new configuration parameter is introduced in SMM to make it possible to control metrics fetching mode.

Cloudera Bug: OPSAPS-57539: Sometimes SMM UI process does not get killed and prevents restarting it

The SMM UI stop script has been improved, so that it will kill the child processes to prevent the SMM UI process from being stuck.

Cloudera Bug: OPSAPS-57468: Hardcoded parcel directory causes failure when non-standard path is used and TLS is enabled

The hardcoded parcel directory path from SMM CSD has been eliminated.

Cloudera Bug: OPSAPS-57423: Upgrade Metadata Directory default value

An incorrect Solr upgrade metadata directory has been fixed.

Cloudera Bug: OPSAPS-57504: Validate base HDFS associated with a compute cluster should have HA enabled

Added a validator to check that the HDFS service in the base cluster associated with a compute cluster is High Availability enabled.

Cloudera Bug: OPSAPS-49148: "Update Hive Metastore NameNodes" invokes metatool for each database

Removed unnecessary executions of the metatool with updateLocation to lower the total execution time and usage of resources for 'Update Hive Metastore NameNodes'.

Cloudera Bug: OPSAPS-57745: SMM UI Server failed to start but status in CM still shows green

Cloudera Manager now correctly displays role status when the SMM UI process fails/stops.

Cloudera Bug: OPSAPS-56456: Application history is lost for Mapreduce apps after upgrade

The log aggregation file controllers suffix configs are automatically changed during the upgrade to a CDP cluster.

Cloudera Bug: OPSAPS-27702: [YARN] Add yarn.nodemanager.linux-container-executor.nonsecure-mode.limit-users as a config

The old buggy ParamSpec was kept to not trigger regression tests. Created a new upgradehandler for 7.2.2 which copies the SV value to the newly introduced ParamSpec during upgrade.

Cloudera Bug: OPSAPS-57394: Create new CM metrics for HBase 2.0 JMX RIT metrics

The following HBASE metrics are now available in Cloudera Manager:

- regions_in_transition_duration_num_ops
- regions_in_transition_duration_min
- regions_in_transition_duration_max
- regions_in_transition_duration_mean

- regions_in_transition_duration_25th_percentile
- regions_in_transition_duration_median
- regions_in_transition_duration_75th_percentile
- regions_in_transition_duration_90th_percentile
- regions_in_transition_duration_95th_percentile
- regions_in_transition_duration_98th_percentile
- regions_in_transition_duration_99th_percentile
- regions_in_transition_duration_99_9th_percentile

Cloudera Bug: OPSAPS-57351: HBase 2.0 JMX SCAN metrics have changed

Due to a HBase 2.0 change, these metrics are no longer available in CM with CDH6+:

- scan_next_rate
- scan_next_size_75th_percentile
- scan_next_size_95th_percentile
- scan_next_size_99th_percentile
- scan_next_size_max
- scan_next_size_mean
- scan_next_size_median
- scan_next_size_min
- 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
- scan_time_75th_percentile
- scan_time_95th_percentile
- scan_time_99th_percentile
- scan_time_max
- scan_time_mean
- scan_time_median
- scan_time_min
- scan_time_rate

Cloudera Bug: OPSAPS-57294: Schema Registry first run fails when multiple Ranger Admin services are configured

The Schema Registry startup script now can handle the case when multiple Ranger Admin services are configured.

Cloudera Bug: OPSAPS-57867: CM Safety-Valve evaluator does not comment out the over-ridden entry

Safety valves for properties files will now override existing values. This is expected to potentially cause staleness and require a restart. Affects CM [7.1.4, 7.2.0) and 7.2.2+.

Cloudera Bug: OPSAPS-57446: Make 'defaultFS' in Core Configuration service optional, fallback to local disk somewhere

The strict validation that requires the Default Filesystem to be specified for the Core Configuration service in base clusters has been removed. Affects all CM versions.

Cloudera Bug: OPSAPS-57618: Add Livy For Spark 3 to the Knox gateway autodiscovery services

Livy For Spark 3 has been added to Knox gateway autodiscovery services.

Cloudera Bug: OPSAPS-57482: JVM GC metrics are not reported for brokers

Detailed GC metrics are now exported for brokers. This change affects CDH >= 7.2.2.

Cloudera Bug: OPSAPS-57444: SMM throws an error if keystore and private key password are not the same

SMM secure configuration now supports non-matching key and keystore passwords. This change affects CDH >= 7.2.2 and CDH >= 7.1.4.

Cloudera Bug: OPSAPS-57587: [SCM] Cluster Template must bar export and import of variables with null values

In Cloudera Manager, the cluster template contains key & value pairs of variables. However, keys without any value(s), get exported into the cluster template's json file. This can happen even if the CM UI exposes the issue by showing configuration warnings. Importing such templates to new clusters also introduces these warnings. Therefore, an export of such templates will require the user to replace the 'null' value. Importing the template with such a key will fail with the appropriate error message.

Cloudera Bug: OPSAPS-57419: [SCM] Disable CM session persistence until CM HA is released

Cloudera Manager's session persistence is disabled by default, until OPSAPS-57366 is fixed.

Cloudera Bug: OPSAPS-57799: [SCM] Handle LDAP's user search DN with multiple spaces

Cloudera Manager fails to parse LDAP DN, OU that contain spaces. This issue has been fixed with OPSAPS-57799.

Cloudera Bug: OPSAPS-57607: redaction.py needs to be sanitise for unicode characters both regex and content

Cloudera Manager Agent failing to redact with the below error is now fixed: "UnicodeDecodeError: 'ascii' codec can't decode byte 0xc3 in position 36."

Cloudera Bug: OPSAPS-57102: [SCM] Diagnostic bundle improvement - Increase number of Archivers and their respective timeouts

Cloudera Manager is now able to anticipate the number of archivers and their respective timeouts based on the size of the cluster it manages. The archivers are used while diagnostic bundle collection occurs. This fix will also provide user to configure the archiver count and heuristically determine scaling factor to set a timeout.

Cloudera Bug: OPSAPS-57532: Impala Thrift profile processing optimization

Monitoring-related performance problems during the execution of Impala queries has been fixed. Memory usage is lowered.

Cloudera Bug: OPSAPS-57990: CM build failing due to Ranger/S3 class conflict

Resolved with removing the unneeded shading.

Cloudera Bug: OPSAPS-57797: HBase restore from ADLS storage filesystem

Fixed an issue where Azure data lake tables could not be restored from backup.

Cloudera Bug: OPSAPS-57534: RMAN historical usage report loses data when a directory is removed from watched directories

Historical Disk Usage reports won't lose the already generated data of the directory after it is set to unwatched.

Cloudera Bug: OPSAPS-57249: Reports Manager unable to index 60G fsimage

Fixed an issue where the previous implementation of the indexing tried to fetch all info about parent-child relationships from the fsimage, to be able to provide the full path of the HDFS nodes. This part never finished for a 60G fsimage.

Cloudera Bug: OPSAPS-55786: Excluding directory from disk usage report has no effect

Directories removed from HDFS will no longer appear in the Current Directory Usage report.

Cloudera Bug: OPSAPS-57720: [SDX upgrade][7.1.0->7.2.2][7.2.0->7.2.2] Create DH cluster fails post upgrade

Cloudera Manager code was missing an upgrade handler for the Hive metastore, so the Hive metastore schema was never upgraded as part of a CDH upgrade. The fix adds a handler.

Cloudera Bug: OPSAPS-57406: Add security related header controls to all Schema Registry responses.

Added the following HTTP headers to ScemaRegistry HTTP responses:

- -Content-Security-Policy
- -XSS-Protection
- -X-Frame options
- -Content-Type-Options
- -Cache-control

Cloudera Bug: OPSAPS-57410: Add Security related headers to SMM Rest API Server responses

Added Security-Related Headers to SMM Rest API responses:

- - Strict-Transport-Security
- - Cache-Control

Cloudera Bug: OPSAPS-57947: Kafka Broker SSL configuration incorrect on HA mode

When deploying a DataHub in High Availability mode, some Ranger and Atlas configurations were not computed correctly, in particular 'atlas.kafka.security.protocol' for Atlas, and the SSL properties and the REST URL for services depending on Ranger.

Cloudera Bug: OPSAPS-57817: Enable Script based Node Attributes to fetch node instance type and hostgroup

Enables script-based node attributes to fetch hostgroup and instance type of the node.

Cloudera Bug: OPSAPS-57277: Add mapred user into yarn.admin.acl

YARN HistoryServer process owned by mapred user has been added into the YARN Admin ACL list, as it has to access job reports from ResourceManager as part of Logs WebService used by YARN UI2.

Cloudera Bug: OPSAPS-57593: Enable Yarn On Cloud from t9000-core

Enables YARN on cloud-related configurations for PUBLIC_CLOUD cluster.

Cloudera Bug: OPSAPS-56714: Possible misinterpretation of Impala query endTime

Impala queries held open after they are finished (e.g. in Hue) now appear on the Impala query monitoring page of Cloudera Manager upon closure, without being logged as "outside acceptance window."

Cloudera Bug: OPSAPS-57448: IDBroker doesn't export correct RDC configs in HA

With this fix, the RDC configs will be correctly exported when IDBroker is in HA mode.

Cloudera Bug: OPSAPS-57109: [SDX patch upgrade] runtime upgrade from 7.1.0 to 7.2.0 fails

Customers can upgrade a CDH cluster from 7.1.0 even with Knox installed.

Cloudera Bug: OPSAPS-57519: Log directory does not work successfully for Knox-IDBroker role

Fixes IDBroker logging via Cloudera Manager.

Cloudera Bug: OPSAPS-57840: [SDX upgrade][7.1.0->7.2.2] create dh failure post upgrade

The error has been resolved with the fix of OPSAPS-57720.

Cloudera Bug: OPSAPS-56088: Improved automatic configuration of YARN, Tez, MR, Hive config parameters based on machine size

Improved automatic configuration of YARN, Tez, MR, Hive config parameters based on machine size.

Cloudera Bug: OPSAPS-57560: "Setup HDFS Data at Rest Encryption" shows as red even with RangerKMS enabled

Fixed an issue where "Setup HDFS Data at Rest Encryption" under CM -> Administration -> Security showed as red even after Ranger KMS was enabled.

Cloudera Bug: OPSAPS-57253: Investigate/Implement a API to create a custom Hive Warehouse Directory

New CM API added:

POST /clusters/{clusterName}/services/{serviceName}/commands/hiveCreateHiveWarehouseExternal, which creates a Hive warehouse external directory with the specified name.

Cloudera Bug: OPSAPS-43909: Exclusion Filter should also apply to Delete Policy

Fixes an issue where the exclusion filter did not apply to the delete policy.

Cloudera Bug: OPSAPS-57495: Custom kerberos principal support for Ranger

Ranger role level principal for Ranger Admin, Ranger Usersync and Ranger Tagsync can now be customised from Cloudera Manager UI.

Cloudera Bug: OPSAPS-56034: Issues with debug level tracing

Fixed Atlas Log threshold change to reflect appropriately. Added atlas-log4j .properties and atlas-env.sh for Atlas Gateway role.

Cloudera Bug: OPSAPS-56130: Ozone Gateway safety valve configs are not part of ozone-site.xml

Ozone configuration Safety values for ozone-conf/ozone-site.xml can now be configured through CM.

Cloudera Bug: OPSAPS-57377: CM Allows addition of multiple role instances for Storage Container Manager

Previously, multiple Ozone Storage Container Manger (SCM) instances could be added in CM. Because SCM does not yet support High Availability, we now only allow one instance to be added per Ozone service.

Cloudera Bug: OPSAPS-57476: Add a new URL in beeline-site.xml that has JDBC config "hiveCreateAsExternalLegacy=true"

This fix gives users the option to to turn on external+purge feature by default while using Hive CLI.

Cloudera Bug: OPSAPS-54413: Hosts API endpoint does not return full health check information

The endpoint /clusters/{clusterName}/hosts now supports all views, with the default view set as SUMMARY. It provides health information of hosts in the cluster for FULL view. Affects CM>=7.2.2, all CDH versions.

Technical Service Bulletins (TSB)

TSB 2022-507 Certificate expiry issue in CDP

For the latest update on this issue, please see the corresponding Knowledge article: TSB 2022-507: Certificate expiry issue in CDP

Known Issues in Cloudera Manager 7.2.2

Learn about the known issues in Cloudera Manager 7.2.2, the impact or changes to the functionality, and the workaround.

OPSAPS-65189: Accessing Cloudera Manager through Knox displays the following error:

Bad Message 431 reason: Request Header Fields Too Large

Workaround: Modify the Cloudera Manager Server configuration /etc/default/cloudera-scm-server file to increase the header size from 8 KB, which is the default value, to 65 KB in the Java options as shown below:

```
export CMF_JAVA_OPTS="...existing options...
-Dcom.cloudera.server.cmf.WebServerImpl.HTTP_HEADER_SIZE_BYTES=
65536
```

```
-Dcom.cloudera.server.cmf.WebServerImpl.HTTPS_HEADER_SIZE_BYTE
S=65536"
```

TSB 2021-472: Customer Advisory for Navigator Metadata Server startup issue

If the Navigator Metadata Server is executing purge, and the clean up process is interrupted, the Navigator Metadata Server will not be able to restart.

Impact

Navigator Metadata Server cannot be restarted if the process is killed or crashes during executing a purge. Error message:

[Update NAV_EXTRACTOR_STATUS set ENABLED_FOR_NEXT_EXTRACTION = 'true']; SQL state [72000]; error code [12899]; ORA-12899: value too large for column "NAVMS"."NAV_EXTRACTOR_STATUS"."ENABLED_FOR_NEXT_EXTRACTION" (actual: 4, maximum: 1; nested exception is java.sql.SQLException: ORA-12899: value too large for column "NAVMS"."NAV_EXTRACTOR_STATUS"."ENABLED_FOR_NEXT_EXTRACTION" (actual: 4, maximum: 1)

Action required

- Upgrade:
  - Cloudera Manager 6.3.4: Request a patch (PATCH-4489).
  - Cloudera Manager 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6 and 7.3.0: Upgrade to a Cloudera Manager version containing the fix.
- Workaround:
  1. Log in to the Navigator Metadata Server database.
  2. Update NAV_MAINTENANCE_HISTORY set STATUS = "INCOMPLETE" where STATUS like 'IN_PROGRESS'.
  3. Update NAV_EXTRACTOR_STATUS set ENABLED_FOR_NEXT_EXTRACTION = 1 where ENABLED_FOR_NEXT_EXTRACTION = 0.
  4. NMS is able to start and extractors are enabled.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article:

Cloudera Customer Advisory-472: Navigator Metadata Server startup issue

TSB 2021-481: Lineage is not extracted with Cloudera Manager 7.2.x and 7.3.1 managing CDH6 or CDH5

Cloudera Manager - Upgrade to Guava 28.1 to avoid CVE-2018-10237 triggered a Guava method version mismatch causing an exception in Navigator Metadata Server. As a result no new lineage and metadata is extracted with Cloudera Manager 7.2.4 and later with CDH6 and CDH5.

Impact

Lineage and metadata are no longer updated in Cloudera Navigator after upgrading to Cloudera Manager 7.2.x or Cloudera Manager 7.3.1 when managing CDH5 or CDH6.

Action required

Upgrade to the patched release of CM 7.3.1 available as PATCH-4822, or to an upcoming version later than 7.3.1. After upgrade, existing entities will have metadata extracted when extraction resumes and no lineage will be permanently lost.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article:

Cloudera Customer Advisory-481: Lineage is not extracted with Cloudera Manager 7.2.x and 7.3.1 managing CDH 6 or CDH 5

TSB 2021-488: Cloudera Manager is vulnerable to Cross-Site-Scripting attack (CVE-2021-29243 and CVE-2021-32482)

Cloudera Manager may be vulnerable to Cross-Site-Scripting vulnerabilities identified by CVE-2021-29243 and CVE-2021-32482. A remote attacker can exploit this vulnerability and execute malicious code in the affected application.

CVE

- CVE-2021-29243
- CVE-2021-32482

Impact

This is an XSS issue. An administrator could be tricked to click on a link that may expose certain information such as session cookies.

Action required

- **Upgrade (recommended)**

Upgrade to a version containing the fix.

- **Workaround**

None

Knowledge article

For the latest update on this issue see the corresponding Knowledge article:

TSB 2021-488: Cloudera Manager vulnerable to Cross-Site-Scripting attack (CVE-2021-29243 and CVE-2021-32482)

TSB 2021-491: Authorization Bypass in Cloudera Manager (CVE-2021-30132/CVE-2021-32483

Cloudera Manager (CM) 7.4.0 and earlier versions have incorrect Access Control in place for certain endpoints. A user who has a knowledge to the direct path of a resource or a URL to call a particular function, can access it without having the proper role granted. The vulnerable endpoints were CVE-2021-30132 /cmf/alerts/config?task= and CVE-2021-32483 /cmf/views/view?viewName=.

CVE

- CVE-2021-30132
  - Alerts config - 4.3 (Medium)
  - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
- CVE-2021-32483
  - Views - 4.3 (Medium)
  - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Impact

A user with read only privilege is able to see configuration information in the UI.

Action required

Upgrade to a version containing the fix.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: TSB 2021-491: Authorization Bypass in Cloudera Manager (CVE-2021-30132 / CVE-2021-32483)