

Cloudera Manager 7.10.1

Release Notes

Date published: 2020-11-30

Date modified: 2023-01-03

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2024. 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 7.10.1 Release Notes.....4

 What's New in Cloudera Manager 7.10.1.....4

 Fixed Issues in Cloudera Manager 7.10.1..... 4

 Known Issues in Cloudera Manager 7.10.1..... 7

Cloudera Manager 7.10.1 Release Notes

Known issues, fixed issues and new features for Cloudera Manager 7.10.1.

What's New in Cloudera Manager 7.10.1

New features and changed behavior for Cloudera Manager 7.10.1.

OPSX 3906: Make ECS default environment name unique in Cloudera Manager.

Added a new SCM parameter called ECS App Domain Unique Regex. The SCM parameter extracts a portion of the app domain name to create the new default environment name. The default ECS environment name that is registered during the installation has changed from “default” to a unique name.

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 makes use of the first layer of the app domain name as the default environment name. For example, with an app Domain name - cloudera-test.cloudera.com and cloudera-test will be used as the default environment name.

Fixed Issues in Cloudera Manager 7.10.1

Fixed issues in Cloudera Manager 7.10.1.

OPSAPS-66539: PathParamspec system resources missing when Ranger Hdfs plugin is enabled in compute clusters .

When Ranger Hdfs plugin is enabled in compute cluster, below pathparamspec system resources are created: - Solr and Hdfs pool directories path - Policy cache directory path

OPSAPS-51761: YARN task failures after upgrading to CDH 6.2.0 (Invalid arguments for cgroups resources: /var/log/hadoop-yarn/container)

Fixed an issue during upgrade in YARN, where the upgraded container-executor binary is not copied due to the container-executor file being used by running applications.

OPSAPS-64733: Setting Hive warehouse directory to Ozone fails because the Ozone filesystem JAR is missing from Cloudera Manager runtime directory.

This issue has been fixed. The Hive metastore warehouse directory and external warehouse directory can be set to Ozone filesystem paths during the first Hive run. The Ozone filesystem JAR is available as part of the hdfs.sh script (in the /opt/cloudera/cm/lib/cdh7 directory).

OPSAPS-66255: Cloudera Manager - GET/clusters/{clusterName}/clientConfig API generating too many directories or files.

Previously, the GET/clusters/{clusterName}/clientConfig API for Spark ran a new command on each invocation, which increased the latency of the API call and created new directories or files under the Cloudera Manager agent process directories. This issue is fixed now.

The latest fix changes the above mentioned behavior and now you can only run the command when there is staleness in Spark2 or Spark3 configurations and later client configuration can be deployed. The files returned for Spark2 and Spark3 are complete files that are collected from a Spark gateway host instead of being generated by Cloudera Manager itself.

OPSAPS-65539: Kudu can not handle multiple Ranger KMS servers

Kudu can now handle HA KMS.

OPSAPS-65267

Cross-site sessions were prohibited in the latest browsers because of SameSite header by default was set to Lax. This issue is fixed now by adding SameSite=None with a secure attribute for the session cookies that are created after login so that cross-site secure cookies are supported.

The secure attribute works only with TLS-configured clusters. You must have a TLS-enabled cluster for cross-site sessions to work.

OPSAPS-65341: ECS and Longhorn UI proxies only read ingress_controller_cert_contents

Previously the ECS and Longhorn UI proxies do not read either from the Cloudera Manager truststore or the system truststore, but only from a Database entry. Due to this reason, your load balancers are unable to access the ECS and Longhorn UI. This latest fix now has the proxies read from both the system truststore and CM truststore. The ingress certificate is also added to the truststore.

OPSAPS-65491: The Skip Inspector button visibility issue when you run the host inspector command

When you run the `host inspector` command, the Run Again button appears first instead of the Skip Inspector button. The Skip Inspector button appears too late. This issue is fixed now and the Skip Inspector button now appears immediately if you want to skip the command.

OPSAPS-65888: The Collect Diagnostic Data button is not active for any date range selected

Previously, when Cloudera Manager is deployed in a timezone different than the user's timezone, it is observed that after selecting a time in the date time picker, the time chosen and the actual time shown do not match with the user's timezone. This issue is now fixed and matches the user's time zone.

OPSAPS-65984: Getting stale configurations issue after upgrading Private Cloud Data Services from 1.4.1 to 1.5.0

Previously after upgrading Private Cloud Data Services from 1.4.1 to 1.5.0, Cloudera Manager was showing stale configurations that are false alerts. This issue is fixed now.

OPSAPS-61519: ECS cluster shows configuration error

Previously, an ECS cluster used to incorrectly show the configuration error: Cluster has stale Kerberos client configuration even though ECS doesn't use Kerberos. This issue is fixed now.

OPSAPS-66023: Error message about an unsupported ciphersuite while upgrading or installing cluster with the latest FIPS compliance

When upgrading or installing a FIPS enabled cluster, Cloudera Manager is unable to download the new CDP parcel from the Cloudera parcel archive.

Cloudera Manager displays the following error message:

```
HTTP ERROR 400 java.net.ConnectException: Unsupported ciphersuite
TLS_EDH_RSA_WITH_3DES_EDE_CBC_SHA
```

This issue is fixed now by correcting the incorrect ciphersuite selection.

OPSAPS-66080: Optimize pattern.compile in CspUtils.java

When Cloudera Manager is running, compiling the regex pattern for CSP multiple times causes other threads to wait, and that results in the slowness of Cloudera Manager. This issue is fixed now.

OPSAPS-66198: On Cloudera Manager UI, the Install Oozie ShareLib command fails to install shared libraries for the Oozie service

On Cloudera Manager UI, the `Install Oozie ShareLib` command fails to install shared libraries for the Oozie service if you configure the Kerberos `krb_krb5_conf_path` file path at the non-default file path. This issue is fixed now.

OPSAPS-66238: ProcessResource API fails with an exception for getting configuration files with multi-level file names

Previously if the user wants to get configuration files under a process directory that contains a multi-level file name, resulting in an API exception. This issue is fixed now.

OPSAPS-66280: Ecs Agent fails to (re)start if Ecs Agent Advanced Configuration Snippet (Safety Valve) for config.yaml is an empty string

Fixed an issue where after clearing the Ecs Agent Advanced Configuration Snippet (Safety Valve) for config.yaml configuration parameter, the Ecs Agent was unable to start.

OPSAPS-66306

When you create a Hive ACID replication policy, the policy does not appear on the Replication Policies page immediately. This issue is fixed.

OPSAPS-66297

Hive ACID replication policies-related issues appear when the source peer becomes unavailable or is deleted as a replication peer. This issue is fixed.

OPSAPS-66068

The Peer not found error appeared during Hive ACID replication policy creation. This issue is fixed.

OPSAPS-66053

Hive ACID replication policies did not appear on the Replication Policies page after policy creation. This issue is fixed.

OPSAPS-66022

When a Hive ACID replication policy run is skipped, the replication policy status incorrectly showed Failed or Error. This issue is fixed.

OPSAPS-65982

When a Hive ACID replication policy was deleted, the error No enum constant com.cloudera.cmf.model.DbReplicationMetric.StatusEnum.FINISHED appeared in Cloudera Manager. This issue is fixed.

OPSAPS-65688

The pre-failover command fails with a FileNotFoundException exception when the bootstrap replication is pending. This issue is fixed.

OPSAPS-65685

After a Hive ACID replication policy fails, the "type" field of replication metrics shows incorrect status. This issue is fixed.

OPSAPS-65410

LDAP authentication error appears during the Hive ACID replication policy creation.

If LDAP authorization is enabled, you must add LDAP_USERNAME and LDAP_PASSWORD fields, and then create the Hive ACID replication policy. Otherwise, an error appears during the replication policy creation.

OPSAPS-64879

Hive ACID replication policies with an empty name do not appear on the Replication Policies page.

Ensure that you provide a unique replication policy name during replication policy creation.

OPSAPS-61643

A Hive replication policy failed during the 'Issue the invalidate metadata command on the Impala shell' step. This issue is fixed.

OPSAPS-63571

Sometimes, entries in the HDFS snapshot-diff report of deleted directories appear as modified. This might raise a FileNotFoundException error.

In this scenario, configure the `com.cloudera.enterprise.distcp.hdfs-snapshot-diff-cleanup.enabled` safety value to address these unexpected entries.

OPSAPS-65732

Hive ACID replication policies failed with a HTTP response code: 401 error because a wrong Kerberos principal was used in the connection string. This issue is fixed.

Known Issues in Cloudera Manager 7.10.1

Known issues in Cloudera Manager 7.10.1.

OPSAPS-68558: Cloudera Manager upgrade fails with the following error: There are 1 active commands of type GetClientConfigFiles

After upgrading from Cloudera Manager 7.9.5 to 7.11.3.0 version, the Cloudera Manager server does not start. Cloudera Manager server log displays an error about **active commands**. This scenario might occur when the Private Cloud Data Service Control Plane is actively issuing requests to Cloudera Manager while performing an upgrade.

Before Cloudera Manager upgrade make sure there are no **active commands** such as `getClientConfig`. If there are any **active commands**, then allow them to complete before kicking off the Cloudera Manager upgrade process.

Post upgrade, inspect the Cloudera Manager server log for the following error message: There are 1 active commands of type `GetClientConfigFiles`. This error might block Cloudera Manager to restart after the upgrade process. If Cloudera Manager restart fails due to the presence of active `getClientConfig` command, then to resolve this issue, perform the following steps:

1. Login to Cloudera Manager database.
2. Search for any active `GetClientConfigFiles` command in `COMMANDS` table.

```
SELECT NAME, ACTIVE , COMMAND_ID FROM COMMANDS WHERE ACTIVE
<> 0 AND NAME='GetClientConfigFiles';
```

3. Update the entry for the `command_id` found in step 2.

```
UPDATE COMMANDS SET active=0,success=false,state='CANCELLED'
where command_id=<command_id>;
```

4. Restart the Cloudera Manager server by running the following command:

```
sudo systemctl restart cloudera-scm-server
```

OPSAPS-67152: Cloudera Manager does not allow you to update some configuration parameters.

Cloudera Manager does not allow you to set to "0" for the `dfs_access_time_precision` and `dfs_name_node_accesstime_precision` configuration parameters.

You will not be able to update `dfs_access_time_precision` and `dfs_namenode_accesstime_precision` to "0". If you try to enter "0" in these configuration input fields, then the field gets cleared off and results in a validation error: This field is required.

To fix this issue, perform the workaround steps as mentioned in the [KB article](#).

If you need any guidance during this process, contact Cloudera support.

OPSAPS-67213: The log files are hitting 403 error.

Accessing the process logs from the command page returns a 403 error: HTTP ERROR 403 Received fatal alert: internal_error The server declined access to the page or resource.

Refreshing the page returns the relevant output.

OPSX-2713: ECS Installation: Failed to perform First Run of services.

If an issue is encountered during the Install Control Plane step of Containerized Cluster First Run, installation will be re-attempted infinitely rather than the command failing.

Since the control plane is installed and uninstalled in a continuous cycle, it is often possible to address the cause of the failure while the command is still running, at which point the next attempted installation should succeed. If this is not successful, abort the First Run command, delete the Containerized Cluster, address the cause of the failure, and retry from the beginning of the Add Cluster wizard. Any nodes that are re-used must be cleaned before re-attempting installation.

OPSX-735: Kerberos service should handle Cloudera Manager downtime

The Cloudera Manager Server in the base cluster must be running in order to generate Kerberos principals for Private Cloud. If there is downtime, you may observe Kerberos-related errors.

Resolve downtime on Cloudera Manager. If you encounter Kerberos errors, you can retry the operation (such as retrying creation of the Virtual Warehouse).

OPSAPS-68629: HDFS HTTPFS GateWay is not able to start with custom krb5.conf location set in Cloudera Manager.

On a cluster with a custom krb5.conf file location configured in Cloudera Manager, HDFS HTTPFS role is not able to start because it does not have the custom Kerberos configuration file setting properly propagated to the service, and therefore it fails with a Kerberos related exception: in thread "main" java.io.IOException: Unable to initialize WebApplicationContext at org.apache.hadoop.http.HttpServer2.start(HttpServer2.java:1240) at org.apache.hadoop.fs.http.server.HttpFSServerWebServer.start(HttpFSServerWebServer.java:131) at org.apache.hadoop.fs.http.server.HttpFSServerWebServer.main(HttpFSServerWebServer.java:162) Caused by: java.lang.IllegalArgumentException: Can't get Kerberos realm at org.apache.hadoop.security.HadoopKerberosName.setConfiguration(HadoopKerberosName.java:71) at org.apache.hadoop.security.UserGroupInformation.initialize(UserGroupInformation.java:329) at org.apache.hadoop.security.UserGroupInformation.setConfiguration(UserGroupInformation.java:380) at org.apache.hadoop.lib.service.hadoop.FileSystemAccessService.init(FileSystemAccessService.java:166) at org.apache.hadoop.lib.server.BaseService.init(BaseService.java:71) at org.apache.hadoop.lib.server.Server.initServices(Server.java:581) at org.apache.hadoop.lib.server.Server.init(Server.java:377) at org.apache.hadoop.fs.http.server.HttpFSServerWebApp.init(HttpFSServerWebApp.java:100) at org.apache.hadoop.lib.servlet.ServerWebApp.contextInitialized(ServerWebApp.java:158) at org.eclipse.jetty.server.handler.ContextHandler.callContextInitialized(ContextHandler.java:1073) at org.eclipse.jetty.servlet.ServletContextHandler.callContextInitialized(ServletContextHandler.java:572) at org.eclipse.jetty.server.handler.ContextHandler.contextInitialized(ContextHandler.java:1002) at org.eclipse.jetty.servlet.ServletHandler.initialize(ServletHandler.java:765) at org.eclipse.jetty.servlet.ServletContextHandler.startContext(ServletContextHandler.java:379) at org.eclipse.jetty.webapp.WebApplicationContext.startWebapp(WebApplicationContext.java:1449) at org.eclipse.jetty.webapp.WebApplicationContext.startContext(WebApplicationContext.java:1414) at org.eclipse.jetty.server.handler.ContextHandler.doStart(ContextHandler.java:916) at org.eclipse.jetty.servlet.ServletContextHandler.doStart(ServletContextHandler.java:288) at org.eclipse.jetty.webapp.WebApplicationContext.doStart(WebApplicationContext.java:524) at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.eclipse.jetty.util.component.ContainerLifeCycle.start(ContainerLifeCycle.java:169) at org.eclipse.jetty.util.component.ContainerLifeCycle.doStart(ContainerLifeCycle.java:117) at org.eclipse.jetty.server.handler.AbstractHandler.doStart(AbstractHandler.java:97) at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.eclipse.jetty.util.component.ContainerLifeCycle.start(ContainerLifeCycle.java:169) at org.eclipse.jetty.server.Server.start(Server.java:423) at org.eclipse.jetty.util.component.ContainerLifeCycle.doStart(ContainerLifeCycle.java:110) at org.eclipse.jetty.server.handler.AbstractHandler.doStart(AbstractHandler.java:97) at org.eclipse.jetty.server.Server.doStart(Server.java:387) at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.apache.hadoop.http.HttpServer2.start(HttpServer2.java:1218) ... 2 more Caused by: java.lang.IllegalArgumentException: KrbException: Cannot locate default realm at java.security.jgss/javax.security.auth.kerberos.KerberosPrincipal.<init>(KerberosPrincipal.java:174) at org.apache.hadoop.security.authentication.util.KerberosU


```
til.getDefaultRealm(KerberosUtil.java:108) at org.apache.hadoop.security.HadoopKerberosName.  
e.setConfiguration(HadoopKerberosName.java:69) ...
```

1. Log in to Cloudera Manager.
2. Select the HDFS service.
3. Select Configurations tab.
4. Search for HttpFS Environment Advanced Configuration Snippet (Safety Valve)
5. Add to or extend the HADOOP_OPTS environment variable with the following value: -
Djava.security.krb5.conf=<the custom krb5.conf location>
6. Click Save Changes.