Cloudera Manager 7.12.0

Release Notes

Date published: 2020-11-30
Date modified: 2024-03-22

https://docs.cloudera.com/

Legal Notice

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

What's New in Cloudera Manager 7.12.0

New features and changed behavior for Cloudera Manager 7.12.0.

New features

Zero Downtime OS upgrade support

Cloudera Manager introduces Zero Downtime OS upgrade feature to improve the upgrade process.

The CDP Runtime services can now intelligently postpone the stopping of role instances until the appropriate time. Thus, ensuring continuous service availability throughout the upgrade process. This improvised process allows for a seamless and uninterrupted availability of services during the OS upgrades.

⚠ **Important:** Currently only KAFKA service supports service availability during OS upgrades.

Changed or updated features

Increased the Cloudera Manager Server default heap memory

Default value of Java maximum heap size for Cloudera Manager Server is increased to 8 GB from 4 GB.

Fixed Issues in Cloudera Manager 7.12.0

Fixed issues in Cloudera Manager 7.12.0.

OPSAPS-69709: Set Sqoop Atlas hook to send notifications synchronously

Sqoop has an Atlas hook which by default runs asynchronously to send notifications to the Atlas server. In certain cases, the Java Virtual Machine (JVM) in which Sqoop is running can shut down before the Kafka notification of the Atlas hook is sent. This can result in lost notifications.

This issue is fixed by ensuring that the notifications are synchronous.

OPSAPS-69759: Multiple TestDFSIO(Mapreduce job) failure during COD ZDU

This issue has been fixed and Mapreduce job failures will no longer occur.

OPSAPS-69340: Dlog4j.configurationFile annotation is not working with the log4j library of the Cloudera Manager Server

The incorrect notation used in defining the log4j configuration file name (which is Dlog4j.configurationFile annotation) is preventing the Cloudera Manager Server from receiving updates made to thelog4j.properties file. This issue is fixed now.

OPSAPS-69485: Invalid mapred-site.xml due to double dash in comments

The string '--' is not allowed in XML comments. Cloudera Manager incorporates values from the safety valve into XML comments. Therefore, XML configuration file generation fails if the safety valve contains '--'.

Cloudera Manager replaces the "--" characters in XML configuration file comments with &#8212 which is the Unicode character of '--'.

OPSAPS-66908: Refresh Cluster command degrades with high node count

The refresh cluster command performance is improved now with asynchronous config generation.

OPSAPS-64516: Unable to clear user's local cache files for YARN in Cloudera Manager

A new YARN command, CleanNmLocalDirCommand, was created to delete the cache files. This command clears, but does not delete the directories under the YARN local directories. This command can only be used if the YARN service is stopped. Users can also now clear the local cache through Cloudera Manager.

OPSAPS-67041: Telemetry Publisher throws FileNotFoundException for Spark application for ifile log

This fix addresses an issue where a modification in the YARN log path caused an inability to access executor logs for Spark in client and cluster modes, and driver logs for Spark in cluster mode through the observability user interface when submitting a Spark job. A similar scenario was observed for Hive as well.

OPSAPS-68500: The cloudera-manager-installer.bin fails to reach Ubuntu 20 repository on the Archive URL due to redirections

Agent Installation with Cloudera Manager on Ubuntu20 platform does not function when the self-installer method (using the installer.bin file) is employed to install Cloudera Manager. The failure mode is that Cloudera Manager Agent installation step will fail with an error message saying "The repository 'https://archive.cloudera.com/p/cm7/7.11.3/ubuntu2004/apt focal-cm7 InRelease' is not signed."

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-67641: Hive ACID replication UX improvement

The **Next Run** column on the Cloudera Manager Replication Replication Policies page was showing **None Scheduled** for recurring Hive ACID replication policy jobs, which is incorrect. The column now displays the correct message.

OPSAPS-68524: Updating OzoneReplicationType in UI

The Listing type option now displays all the available options where you can choose a replication method to replicate Ozone data using Ozone replication policies.

OPSAPS-69063: Concurrent policy creation to multiple targets

Sometimes, standard error or standard output retrieval of Cloudera Manager commands would fail because of a Java-related issue which affected the HTTPS connections with TLSv1.3 protocol. This resulted in different failures when the HBase replication commands were run remotely from the destination cluster on the source cluster. This issue is now resolved.

OPSAPS-68995: Convert some DistCp feature checks from CM version checks to feature flags

To ensure interoperability between different cumulative hotfixes (CHF), the NUM_FETCH_THREADS, DELETE_LATEST_SOURCE_SNAPSHOT_ON_JOB_FAILURE, and RAISE_SNAPSHOT_DIFF_FAILURES DistCp features must be published as feature flags.

OPSAPS-69481: Some Kafka connect metrics missing from Cloudera Manager due to conflicting definitions

Cloudera Manager now registers kafka_connect_connector_task_metrics_batch_size_avg and kafka_connect_connector_task_metrics_batch_size_max metrics correctly.

Known Issues in Cloudera Manager 7.12.0

Known issues in Cloudera Manager 7.12.0.

OPSAPS-69487: Failed to start role <role-name>-<role-id> of <service-name> in cluster <cluster-name>. This role requires the following additional parcels to be activated before it can start: <parcel-name>

During a patch upgrade or any other cluster upgrade, there is a phase where the upgrade is nearly completed, but the start of upgraded services/roles occasionally fails. This issue arises because the Cloudera Manager's agent operation gets delayed, consequently it provides incomplete information during role startup which results in role startup failure.

Use the Retry functionality from the control plane.

Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.12.0 (Cloudera Runtime 7.2.18)

Common Vulnerabilities and Exposures (CVE) that are fixed in this release.

- CVE-2022-41915
- CVE-2022-46364
- CVE-2022-46363
- CVE-2023-36478
- CVE-2023-26048
- CVE-2023-26049
- CVE-2023-40167
- CVE-2023-36479
- CVE-2023-41900
- CVE-2014-125087
- CVE-2023-1436
- CVE-2021-28165
- CVE-2022-2048
- CVE-2020-27223
- CVE-2021-28169
- CVE-2021-34428
- CVE-2021-28163
- CVE-2022-2047
- CVE-2023-1370
- CVE-2021-35515
- CVE-2021-35516
- CVE-2021-35517
- CVE-2021-36090
- CVE-2023-25613
- CVE-2023-3635
- CVE-2022-1471
- CVE-2023-34453
- CVE-2023-34454
- CVE-2023-34455
- CVE-2022-31692
- CVE-2023-34034

- CVE-2022-31690
- CVE-2020-13936
- CVE-2019-14887
- CVE-2022-45688

Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.12.0 release.

Cloudera Manager 7.12.0.500

Know more about the Cloudera Manager 7.12.0.500 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.500 service pack release.

This cumulative hotfix was released on December 18, 2024.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.500 (version: 7.12.0.500-60783757):

OPSAPS-71436: Telemetry publisher test altus connection fails for Cloudera Manager 7.11.3 hotfix (CHF6, 7, and 8) versions

An error occurred while running the Test Altus Connection action for Telemetry Publisher. This issue is fixed now.

OPSAPS-71090: The spark.*.access.hadoopFileSystems gateway properties are not propagated to Livy.

Added new properties for configuring Spark 2 (spark.yarn.access.hadoopFileSystems) and Spark 3 (spark.kerberos.access.hadoopFileSystems) that propagate to Livy.

OPSAPS-71005: RemoteCmdWork is using a singlethreaded executor

By default, Replication Manager runs the remote commands for a replication policy through a single-thread executor. You can search and enable the enable_multithreaded_remote_cmd_executor property in the target Cloudera Manager Administration Settings page to run future replication policies through the multi-threaded executor. This action improves the processing performance of the replication workloads.

Additionally, you can also change the multithreaded_remote_cmd_executor_max_threads and multithreaded_remote_cmd_executor_keepalive_time properties to fine-tune the replication policy performance.

OPSAPS-72153: Invalid signature when trying to create tags in Atlas through Knox

Atlas, SMM UI, and SCHEMA-REGISTRY throw 500 error in FIPS environment.

This issue is fixed now.

OPSAPS-70983: Hive replication command for Sentry to Ranger replication works as expected

The Sentry to Ranger migration during the Hive replication policy run from CDH 6.3.x or higher to CDP Public Cloud 7.3.0.1 or higher is successful.

OPSAPS-70583: File Descriptor leak in Cloudera Manager

Unable to create NettyTransceiver due to Avro library upgrade which leads to File Descriptor leak. File Descriptor leak occurs in Cloudera Manager when a service tries to talk with Event Server over Avro. This issue is fixed now.

OPSAPS-68845: Cloudera Manager Server fails to start after the Cloudera Manager upgrade

Starting from the Cloudera Manager 7.11.3 version up to the Cloudera Manager 7.11.3 CHF7 version, the Cloudera Manager Server fails to start after the Cloudera Manager upgrade due to Navigator user roles improperly handled in the upgrade in some scenarios. This issue is fixed now by removing the extra Navigator roles.

OPSAPS-69996: HBase snapshot creation in Cloudera Manager works as expected

During the HBase snapshot creation process, the snapshot create command sometimes tries to create the same snapshot twice because of an unhandled OptimisticLockException during the database write operation. This resulted in intermittent HBase snapshot creation failures. The issue is now fixed.

OPSAPS-71647: Ozone replication fails for incompatible source and target Cloudera Manager versions during the payload serialization operation

Replication Manager now recognizes and annotates the required fields during the payload serialization operation. For the list of unsupported Cloudera Manager versions that do not have this fix, see Preparing clusters to replicate Ozone data.

OPSAPS-66459: Enable concurrent Hive external table replication policies with the same cloud root

When the HIVE_ALLOW_CONCURRENT_REPLICATION_WITH_SAME_CLOUD_ROOT_PATH feature flag is enabled, Replication Manager can run two or more Hive external table replication policies with the same cloud root path concurrently.

For example, if two Hive external table replication policies have s3a://bucket/hive/data as the cloud root path and the feature flag is enabled, Replication manager runs these policies concurrently.

By default, this feature flag is disabled. To enable the feature flag, contact your Cloudera account team.

OPSAPS-69782: Exception appears if the peer Cloudera Manager's API version is higher than the local cluster's API version

HBase replication using HBase replication policies in CDP Public Cloud Replication Manager between two Data Hubs/COD clusters succeed as expected when all the following conditions are true:

- The destination Data Hub/COD cluster’s Cloudera Manager version is 7.9.0-h7 through 7.9.0-h9 or 7.11.0-h2 through 7.11.0-h4, or 7.12.0.0.
- The source Data Hub/COD cluster's Cloudera Manager major version is higher than the destination cluster's Cloudera Manager major version.
- The Initial Snapshot option is chosen during the HBase replication policy creation process and/or the source cluster is already participating in another HBase replication setup as a source or destination with a third cluster.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.500 hotfix.

CVEs	Package Name
CVE-2021-29425	commons-io
CVE-2021-28168	jersey-common
CVE-2020-11971	Apache Camel
CVE-2020-13697	Nanohttpd
CVE-2022-21230	Nanohttpd
CVE-2024-29736	Apache cxf
CVE-2024-32007	Apache cxf

CVEs	Package Name
CVE-2022-1415	Drools
CVE-2021-41411	Drools
CVE-2017-7536	Hibernate-validator
CVE-2022-41853	Hasqldb
CVE-2024-1597	Postgresql
CVE-2022-34169	Xalan
CVE-2023-43642	Snappy-java
CVE-2024-38808	Spring Framework

The repositories for Cloudera Manager 7.12.0.500 are listed in the following table:

Table 1: Cloudera Manager 7.12.0.500

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.500-60783757/redhat8/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.500-60783757/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.400

Know more about the Cloudera Manager 7.12.0.400 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.400 service pack release.

This cumulative hotfix was released on October 4, 2024.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.400 (version: 7.12.0.400-57266911):

OPSAPS-71090: The spark.*.access.hadoopFileSystems gateway properties are not propagated to Livy.

Added new properties for configuring Spark 2 (spark.yarn.access.hadoopFileSystems) and Spark 3 (spark.kerberos.access.hadoopFileSystems) that propagate to Livy.

OPSAPS-71005: RemoteCmdWork is using a singlethreaded executor

By default, Replication Manager runs the remote commands for a replication policy through a single-thread executor. You can search and enable the enable_multithreaded_remote_cmd_executor property in the target Cloudera Manager Administration Settings page to run future replication policies through the multi-threaded executor. This action improves the processing performance of the replication workloads.

Additionally, you can also change the multithreaded_remote_cmd_executor_max_threads and multithreaded_remote_cmd_executor_keepalive_time properties to fine-tune the replication policy performance.

OPSAPS-70983: Hive replication command for Sentry to Ranger replication works as expected

The Sentry to Ranger migration during the Hive replication policy run from CDH 6.3.x or higher to CDP Public Cloud 7.3.0.1 or higher is successful.

OPSAPS-70583: File Descriptor leak in Cloudera Manager

Unable to create NettyTransceiver due to Avro library upgrade which leads to File Descriptor leak. File Descriptor leak occurs in Cloudera Manager when a service tries to talk with Event Server over Avro. This issue is fixed now.

OPSAPS-68845: Cloudera Manager Server fails to start after the Cloudera Manager upgrade

Starting from the Cloudera Manager 7.11.3 version up to the Cloudera Manager 7.11.3 CHF7 version, the Cloudera Manager Server fails to start after the Cloudera Manager upgrade due to Navigator user roles improperly handled in the upgrade in some scenarios. This issue is fixed now by removing the extra Navigator roles.

OPSAPS-69996: HBase snapshot creation in Cloudera Manager works as expected

During the HBase snapshot creation process, the snapshot create command sometimes tries to create the same snapshot twice because of an unhandled OptimisticLockException during the database write operation. This resulted in intermittent HBase snapshot creation failures. The issue is now fixed.

The repositories for Cloudera Manager 7.12.0.400 are listed in the following table:

Table 2: Cloudera Manager 7.12.0.400

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.400-57266911/redhat8/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.400-57266911/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.300

Know more about the Cloudera Manager 7.12.0.300 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.300 service pack release.

This cumulative hotfix was released on August 30, 2024.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.300 (version: 7.12.0.300-55584068):

OPSAPS-70976: The previously hidden real-time monitoring properties are now visible in the Cloudera Manager UI:

The following properties are now visible in the Cloudera Manager UI:

- enable_observability_real_time_jobs
- enable_observability_metrics_dmp

OPSAPS-70821: The Time To Live for Solr Collection of Ranger Audits configuration issue in Ranger

The warning message text which appeared when the Time To Live For Solr Collection Of Ranger Audits configuration had value more than 30 days. This was not proper and did not have the option to suppress the warning.

The issue is fixed now. The warning message text is fixed and an option to suppress the warning is also included.

OPSAPS-70655: The hadoop-metrics2.properties file is not getting generated into the ranger-rms-conf folder

The hadoop-metrics2.properties file was getting created in the process directory conf folder, for example, conf/hadoop-metrics2.properties, whereas the directory structure in Ranger RMS should be {process_directory}/ranger-rms-conf/hadoop-metrics2.properties.

The issue is fixed now. The directory name is changed from conf to ranger-rms-conf, so that the hadoop-metrics2.properties file gets created under the correct directory structure.

OPSAPS-68252: The `Ranger RMS Database Full Sync` command is not visible on cloud clusters

The `Ranger RMS Database Full Sync` command was not visible on any cloud cluster. Also, it was needed to investigate the minimum user privilege required to see the `Ranger RMS Database Full Sync` command on the UI.

The issue is fixed now. The command definition on service level in Ranger RMS has been updated after which the command is visible on the UI. The minimum user privilege required to see this command is EnvironmentAdmin.

The repositories for Cloudera Manager 7.12.0.300 are listed in the following table:

Table 3: Cloudera Manager 7.12.0.300

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.300-55584068/redhat8/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm-public/7.12.0.300-55584068/redhat8/yum/cloudera-manager.repo`