Cloudera Manager 7.12.0

Release Notes

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

https://docs.cloudera.com/

Legal Notice

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 7.12.0.1101

Know more about the Cloudera Manager 7.12.0.1101 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.1101 service pack release.

This cumulative hotfix was released on July 31, 2025.

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

Following are the list of known issues and their corresponding workarounds for Cloudera Manager 7.12.0.1101 (version: 7.12.0.1101-68678967):
OPSAPS-72335: HDFS roles does not consume extra_jvm_opts

The extra_jvm_opts configuration in Cloudera Manager is not picked by the hdfs.sh script. Any operations performed using this script will not have access to the extra JVM options that might have been added. This does not affect HDFS service and anything performed directly in HDFS will have the extra opts applied.

None

Avoid using hdfs.sh script and prefer using HDFS commands directly. Alternatively if any command is absolutely required, you can modify the hdfs.sh script to directly include the necessary opts. For example, to add jdk.tls.maxHandshakeMessageSize option to the script before running com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDirUtil command, run the following bash ciommand:

```
if [[ $(grep -c maxHandshakeMessageSize /opt/cloudera/cm-agent/s
ervice/hdfs/hdfs.sh) -eq 0 ]]
then
sed -i.bak 's|exec ${JAVA} ${MKDIR_JAVA_OPTS} -cp ${MKDIR_CLASSPA
TH} com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDirUtil ${D
IR} ${USER} ${GROUP} ${PERMS} ${MKDIR_FLAGS}|exec ${JAVA} ${MKDI
R_JAVA_OPTS} -Djdk.tls.maxHandshakeMessageSize=262144 -cp ${MKDI
R_CLASSPATH} com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDi
rUtil ${DIR} ${USER} ${GROUP} ${PERMS} ${MKDIR_FLAGS}|' /opt/clo
udera/cm-agent/service/hdfs/hdfs.sh
fi
```

This code snippet direct modifies the script to include the required options and can be further modified to add any number of such arguments as necessary.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.1101 (version: 7.12.0.1101-68678967):
OPSAPS-73921: The Proxy server settings are not working correctly for the Telemetry Publisher in Cloudera Manager versions 7.11.3 and higher.

The Proxy server issues are resolved by updating the cdp-sdk-java artifact's version. This issue is now resolved.

OPSAPS-73791: Telemetry Publisher exhibited incorrect behaviour during job uploads by accepting a Status Code 503 response and marking logs as successfully exported.

The issue is now resolved. Telemetry Publisher now treats only Status Code 200 as successful. For non-200 status codes, Telemetry Publisher will now log an error message.

OPSAPS-72739: Snappy native library loading failure

Snappy native library loading fail in certain cluster configurations. This occurs because Snappy attempts to locate its .so files in /var/lib/hive.

This issue is now fixed.

OPSAPS-60642: Host header injection issue on /j_spring_security_check internal endpoint

/j_spring_security_check is internal endpoint which is vulnerable to Host header injection. This issue occurs if the user disabled PREVENT_HOST_HEADER_INJECTION feature flag.

Host header injection: In an incoming HTTP request, web servers often dispatch the request to the target virtual host based on the value supplied in the Host header. Without proper validation of the header value, the attacker can supply invalid input to cause the web server to:

- Dispatch requests to the first virtual host on the list
- Redirect to an attacker-controlled domain
- Perform web cache poisoning
- Manipulate password reset functionality

This issue is resolved now by adding Feature Flag PREVENT_HOST_HEADER_INJECTION to prevent host header injection vulnerability on /j_spring_security_check internal endpoint. This feature flag is by default enabled and it enables additional logic to block potential Host Header Injection attacks targeting the /j_spring_security_check endpoint in Cloudera Manager.

OPSAPS-73585: Cloudera Observability does not report Spark workloads when Spark event log compression is enabled by setting spark.eventLog.compress enabled to true.

Cloudera Observability now accurately handles compressed event log files. This issue is now resolved.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.1101 hotfix.

CVEs	Package Name
CVE-2019-10172	Jackson-mapper-asl
CVE-2024-22201	Jetty
CVE-2025-31672	Apache POI
CVE-2024-38820	Spring Framework
CVE-2025-22228	Spring Security

The repositories for Cloudera Manager 7.12.0.1101 are listed in the following table:

Table 1: Cloudera Manager 7.12.0.1101

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.1101-68678967/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.1101-68678967/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.1000

Know more about the Cloudera Manager 7.12.0.1000 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.1000 service pack release.

This cumulative hotfix was released on June 4, 2025.

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

Following are the list of known issues and their corresponding workarounds for Cloudera Manager 7.12.0.1000 (version: 7.12.0.1000-66317008):

OPSAPS-72335: HDFS roles does not consume extra_jvm_opts

The extra_jvm_opts configuration in Cloudera Manager is not picked by the hdfs.sh script. Any operations performed using this script will not have access to the extra JVM options that might have been added. This does not affect HDFS service and anything performed directly in HDFS will have the extra opts applied.

None

Avoid using hdfs.sh script and prefer using HDFS commands directly. Alternatively if any command is absolutely required, you can modify the hdfs.sh script to directly include the necessary opts. For example, to add jdk.tls.maxHandshakeMessageSize option to the script before running com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDirUtil command, run the following bash ciommand:

```
if [[ $(grep -c maxHandshakeMessageSize /opt/cloudera/cm-agent/service/hdfs/hdfs.sh) -eq 0 ]]
then
sed -i.bak 's|exec ${JAVA} ${MKDIR_JAVA_OPTS} -cp ${MKDIR_CLASSPATH} com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDirUtil ${DIR} ${USER} ${GROUP} ${PERMS} ${MKDIR_FLAGS}|exec ${JAVA} ${MKDIR_JAVA_OPTS} -Djdk.tls.maxHandshakeMessageSize=262144 -cp ${MKDIR_CLASSPATH} com.cloudera.cmf.cdhclient.common.hdfs.CreateHdfsDirUtil ${DIR} ${USER} ${GROUP} ${PERMS} ${MKDIR_FLAGS}|' /opt/cloudera/cm-agent/service/hdfs/hdfs.sh
fi
```

This code snippet direct modifies the script to include the required options and can be further modified to add any number of such arguments as necessary.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.1000 (version: 7.12.0.1000-66317008):

OPSAPS-73123: Ranger RMS server shows as healthy without being accessible

Ranger RMS service is not getting initialized due to some issues, but at the same time Ranger RMS service appears as healthy on Cloudera Manager.

The issue is fixed now. The changes to support Ranger RMS Canary, which can check for the availability of Ranger RMS and update the status on Cloudera Manager, have been added.

OPSAPS-73529: Backported the ability to disable ZooKeeper clientPort by allowing zero value

The user is now able to set 0 value (disable) to ZooKeeper's clientPort setting.

OPSAPS-73165: When Ranger is enabled, Telemetry Publisher fails to export Hive payloads from Data Hub due to the missing Ranger client dependencies in the Telemetry Publisher classpath.

This issue has been resolved by adding the necessary dependencies to the classpath.

OPSAPS-73370: Cloudera Observability does not report Spark workloads when Spark event log compression is enabled by setting spark.eventLog.compress enabled to true.

Cloudera Observability now accurately handles compressed event log files. This issue is now resolved.

OPSAPS-72978: The getUsersFromRanger API parameter truncates the user list after 200 items

The Cloudera Manager API endpoint v58/clusters/[***CLUSTER***]/services/[***SERVICE***]/commands/getUsersFromRanger API endpoint no longer truncates the list of returned users at 200 items.

OPSAPS-71459: Commands continue to run after Cloudera Manager restart

Some remote replication commands continue to run endlessly even after a Cloudera Manager restart operation. This issue is fixed.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.1000 hotfix.

CVEs	Package Name
CVE-2022-45688	org.json
CVE-2024-53990	async-http-client
CVE-2023-33202	Bouncycastle
CVE-2024-34447	Bouncycastle
CVE-2024-29857	Bouncycastle
CVE-2024-30171	Bouncycastle
CVE-2023-33201	Bouncycastle
CVE-2024-30172	Bouncycastle
CVE-2023-34442	Apache Camel
CVE-2025-27636	Apache Camel
CVE-2023-5072	org.json
CVE-2022-1471	Snakeyaml
CVE-2024-47554	Commons-io

The repositories for Cloudera Manager 7.12.0.1000 are listed in the following table:

Table 2: Cloudera Manager 7.12.0.1000

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.1000-66317008/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.1000-66317008/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.900

Know more about the Cloudera Manager 7.12.0.900 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.900 service pack release.

This cumulative hotfix was released on April 28, 2025.

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

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.900 (version: 7.12.0.900-65149388):

OPSAPS-72632: Cloudera Manager - Stale service restart API call is failing

When there is a configuration change for the Cloudera Management Service (CMS), process staleness detection for the CMS does not work. This issue is fixed now.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.900 hotfix.

CVEs	Package Name
CVE-2025-23184	Apache CXF
CVE-2021-28170	javax.el
CVE-2024-47072	XStream
CVE-2023-24998	Apache Commons FileUpload
CVE-2012-5783	Apache Commons HttpClient
CVE-2014-3577	Apache Commons HttpClient
CVE-2020-13956	Apache Commons HttpClient
CVE-2015-5262	Apache Commons HttpClient
CVE-2012-6153	Apache Commons HttpClient

The repositories for Cloudera Manager 7.12.0.900 are listed in the following table:

Table 3: Cloudera Manager 7.12.0.900

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.900-65149388/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.900-65149388/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.800

Know more about the Cloudera Manager 7.12.0.800 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.800 service pack release.

This cumulative hotfix was released on March 11, 2025.

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

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.800 (version: 7.12.0.800-63672996):

OPSAPS-72809: Ranger policy script for Knox fails due to double quotation marks

The Ranger policy script for Knox (setupRanger.sh) fails, because the CSD_JAVA_OPTS parameters are enclosed by double quotation marks in the script. The issue is fixed now.

OPSAPS-71933: Telemetry Publisher is unable to publish Spark event logs to Observability when multiple History Servers are set up in the Spark service.

This issue is now resolved by adding the support for multiple Spark History Server deployments in Telemetry Publisher.

OPSAPS-72767: `Install Oozie ShareLib` Cloudera Manager command fails on FIPS and FedRAMP clusters

The `Install Oozie ShareLib` command using Cloudera Manager fails to execute on FIPS and FedRAMP clusters. This issue is fixed now.

OPSAPS-71566: The polling logic of RemoteCmdWork goes down if the remote Cloudera Manager goes down

When the remote Cloudera Manager goes down or when there are network failures, the RemoteCmdWork stops to poll. To ensure that the daemon continues to poll even when there are network failures or if the Cloudera Manager goes down, you can set the remote_cmd_network_failure_max_poll_count=*[*** ENTER REMOTE EXECUTOR MAX POLL COUNT***]* parameter on the Cloudera Manager Administration Settings page. Note that the actual timeout is provided by a piecewise constant function (step function) where the breakpoints are: 1 through 11 is 5 seconds, 12 through 17 is 1 minute, 18 through 35 is 2 minutes, 36 through 53 is 5 minutes, 54 through 74 is 8 minutes, 75 through 104 is 15 minutes, and so on. Therefore when you enter 1, the polling continues for 5 seconds after the Cloudera Manager goes down or after a network failure. Similarly when you set it 75, the polling continues for 15 minutes.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.800 hotfix.

CVEs	Package Name
CVE-2023-0833	okhttp
CVE-2021-0341	okhttp
CVE-2023-48795	sshj
CVE-2022-21699	IPython
CVE-2015-5607	IPython
CVE-2014-3429	IPython
CVE-2015-4707	IPython
CVE-2024-3651	Idna

The repositories for Cloudera Manager 7.12.0.800 are listed in the following table:

Table 4: Cloudera Manager 7.12.0.800

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.800-63672996/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.800-63672996/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.700

Know more about the Cloudera Manager 7.12.0.700 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.700 service pack release.

This cumulative hotfix was released on February 13, 2025.

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

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.700 (version: 7.12.0.700-62379925):

OPSAPS-67498: The Replication Policies page takes a long time to load

To ensure that the Cloudera Manager Replication Manager Replication Policies page loads faster, new query parameters have been added to the internal policies that fetch the REST APIs for the page which improves pagination. Replication Manager also caches internal API responses to speed up the page load.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.700 hotfix.

CVEs	Package Name
CVE-2023-52428	Nimbus-jose-jwt
CVE-2022-22965	Spring Framework

CVEs	Package Name
CVE-2023-20860	Spring Framework
CVE-2022-22950	Spring Framework
CVE-2022-22971	Spring Framework
CVE-2023-20861	Spring Framework
CVE-2023-20863	Spring Framework
CVE-2022-22968	Spring Framework
CVE-2022-22970	Spring Framework
CVE-2021-22060	Spring Framework
CVE-2021-22096	Spring Framework
CVE-2024-38821	Spring Security
CVE-2024-38816	Spring Framework

The repositories for Cloudera Manager 7.12.0.700 are listed in the following table:

Table 5: Cloudera Manager 7.12.0.700

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.700-62379925/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.700-62379925/redhat8/yum/cloudera-manager.repo`

Cloudera Manager 7.12.0.600

Know more about the Cloudera Manager 7.12.0.600 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.18.600 service pack release.

This cumulative hotfix was released on January 23, 2025.

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

Following are the list of fixed issues that were shipped for Cloudera Manager 7.12.0.600 (version: 7.12.0.600-61784706):

OPSAPS-70449: After creating a new Dashboard from the Cloudera Manager UI, the Chart Title field was allowing Javascript as input

In Cloudera Manager UI, while creating a new plot object, a **Chart Title** field allows Javascript as input. This allows the user to execute a script, which results in an XSS attack. This issue is fixed now.

OPSAPS-72254: FIPS Failed to upload Spark example jar to HDFS in cluster mode

Fixed an issue with deploying the Spark 3 Client Advanced Configuration Snippet (Safety Valve) for spark3-conf/spark-env.sh.

For more information, see Added a new Cloudera Manager configuration parameter spark_pyspark_executable_path to Livy for Spark 3.

New features and changed behavior for Cloudera Manager 7.12.0.600 (version: 7.12.0.600-61784706): Added a new Cloudera Manager configuration parameter spark_pyspark_executable_path to Livy for Spark 3.

In Cloudera Manager Agent 7.13.1 and higher versions, a new Cloudera Manager configuration parameter spark_pyspark_executable_path is added to Livy for Spark 3 service.

The value of spark_pyspark_executable_path for Livy must sync with the value of the Spark 3 service's spark_pyspark_executable_path parameter in Cloudera Manager.

Important:

If the PYSPARK_PYTHON/PYSPARK_DRIVER_PYTHON environment variables are not set in spark-env.sh, then the default value of these variables will be the value of the spark_pyspark_executable_path Cloudera Manager property.

The default value of spark_pyspark_executable_path is /opt/cloudera/cm-agent/bin/python.

Summary: The Livy proxy user is taken from Livy for Spark 3's configuration.

Previous behavior:

The custom Kerberos principal configuration was updated via the Livy service.

New behavior:

The Livy proxy user is taken from Livy for Spark 3's configuration, as the Livy service has been replaced with Livy for Spark3 in Cloudera Private Cloud Public Cloud version 7.3.1.

Fixed Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.12.0.600 hotfix.

CVEs	Package Name
CVE-2024-37891	urllib3
CVE-2023-43804	urllib3
CVE-2021-33503	urllib3
CVE-2020-26137	urllib3
CVE-2024-21634	Ion-Java
CVE-2024-25710	Commons-Compress
CVE-2024-26308	Commons-Compress
CVE-2024-36114	Aircompressor
CVE-2020-13949	libthrift
CVE-2018-1320	libthrift
CVE-2019-0205	libthrift
CVE-2019-0210	libthrift
CVE-2018-11798	libthrift

The repositories for Cloudera Manager 7.12.0.600 are listed in the following table:

Table 6: Cloudera Manager 7.12.0.600

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.600-61784706/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.12.0.600-61784706/redhat8/yum/cloudera-manager.repo`

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

CVEs	Package Name
CVE-2024-29736	Apache cxf
CVE-2024-32007	Apache cxf
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 7: 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 8: 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 9: 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`