Cloudera Manager 7.7.1

Release Notes

Date published: 2020-11-30
Date modified: 2024-01-18

CLOUDERA

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

Cloudera Manager 7.7.3 Release Notes

Known issues, fixed issues and new features for Cloudera Manager and CDP Private Cloud.

What's New in Cloudera Manager 7.7.3

New features and changed behavior for Cloudera Manager 7.7.3 and cumulative hotfixes.

Note: Cloudera Manager 7.7.3 and the associated cumulative hotfixes will not work with Python 2.7.

Platform support for Cloudera Manager 7.7.3-CHF2

The following operating systems are supported when using Python 3.8 with the Cloudera Manager agents:

- RHEL 8.4
- RHEL 8.6
- RHEL 7.9

Important: Cloudera recommends you to use Cloudera Manager 7.7.3-CHF2 with Cloudera Runtime 7.1.8-CHF3 as this includes a critical Apache Impala fix.

For a list of issues fixed in Cloudera Manager 7.7.3-CHF2, see Cloudera Manager 7.7.3 Cumulative hotfix 2.

Platform support updates for Cloudera Manager 7.7.3-CHF1

The following operating systems are now supported when using Python 3.8 with the Cloudera Manager agents:

- RHEL 8.4
- RHEL 8.6
- RHEL 7.9

For a list of issues fixed in Cloudera Manager 7.7.3-CHF1, see Cloudera Manager 7.7.3 Cumulative hotfix 1.

Platform support updates for Cloudera Manager 7.7.3

Cloudera Manager 7.7.3 adds support for using Python 3.8 with the Cloudera Manager agents. Python 3.8 is only supported with the following operating systems:

- RHEL 8.6
- RHEL 8.4

You must install Python 3.8 on all hosts before upgrading to Cloudera Manager 7.7.3. See Installing Python 3.8 on RHEL 8 for Cloudera Manager 7.7.3.

Fixed Issues in Cloudera Manager 7.7.3

Fixed issues in Cloudera Manager 7.7.3.

Cloudera Bug: OPSAPS-64287 New configuration parameter for Data Analytics Studio to configure header size.

Data Analytics Studio (DAS) has a new, optional parameter named das_application_connector_configs to configure header size.

Cloudera Bug: OPSAPS-63881 Permissions of user directories under /var/lib/ is 700 on RHEL 8.4

This issue applies only when RHEL 8.4 or higher is used. In these versions the /etc/login.defs file has HOME_MODE configured with 700 permissions. Due to this, service directories were incorrectly created with 700 permissions.

Known Issues in Cloudera Manager 7.7.3

Known issues in Cloudera Manager 7.7.3

OPSAPS-65691: Cloudera Manager upgrade from 7.6.7 version fails with an ApiException error

While upgrading Cloudera Manager from Cloudera Manager 7.6.7 to Cloudera Manager 7.7.3, the upgrade failed with the following error message: ApiException: Expected boolean. Got END_OBJECT (error 400).

The following error is also logged in Cloudera Manager server log: scm-web-198:com.cloudera.server.web.cmf.home.SystemHealth: HealthInfo Exception:Exception occurred inside setter of com.cloudera.cmf.model.DbProcess.specialFileInfoForDb

Upgrade to the Cloudera Manager 7.7.3 CHF4 or later versions where this issue is fixed.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

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_namenode_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.

Cloudera bug: OPSAPS-59764: Memory leak in the Cloudera Manager agent while downloading the parcels.

When using the M2Crpyto library in the Cloudera Manager agent to download parcels causes a memory leak.

The Cloudera Manager server requires parcels to install a cluster. If any of the URLs of parcels are modified, then the server provides information to all the Cloudera Manager agent processes that are installed on each cluster host.

The Cloudera Manager agent then starts checking for updates regularly by downloading the manifest file that is available under each of the URLs. However, if the URL is invalid or not reachable to download the parcel, then the Cloudera Manager agent shows a 404 error message and the memory of the Cloudera Manager agent process increases due to a memory leak in the file downloader code of the agent.

To prevent this memory leak, ensure all URLs of parcels in Cloudera Manager are reachable. To achieve this, delete all unused and unreachable parcels from the Cloudera Manager parcels page.

Cloudera bug: OPSAPS-66235 Diagnostic bundle missing host statistics

Diagnostic bundles do not include host statistics. The following error message displays in the command output: Collect Host Statistics sub-command has failed.

None

Cloudera bug: OPSAPS-65243 Diagnostic data collection for YARN fails

Selecting Collect Diagnostic Data from the YARN Applications page fails to generate the diagnostic data.

None

Cloudera bug: OPSAPS-65269 Hosts report no heartbeat after upgrading to Cloudera Manager 7.7.3 and then rolling back to Cloudera Manager 7.7.1.

After upgrading Cloudera Manager 7.7.1 to 7.7.3 and then rolling back to 7.7.1 Cloudera Manager may report no heartbeat from one or more hosts and also reports bad health for services.

Reboot the hosts.

Cloudera bug: 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"
```

OPSAPS-65213: Ending the maintenance mode for a commissioned host with either an Ozone DataNode role or a Kafka Broker role running on it, might result in an error.

You may see the following error if you end the maintenance mode for Ozone and Kafka services from Cloudera Manager when the roles are not decommissioned on the host.

```
Execute command Recommission and Start on service OZONE-1
Failed to execute command Recommission and Start on service OZ
ONE-1
Recommission and Start
Command Recommission and Start is not currently available for e
xecution.
```

To resolve this issue, use the API support feature to take the host out of maintenance mode.

1. Log into Cloudera Manager as an Administrator.
2. Go to Hosts All Hosts .

3. Select the host for which you need to end the maintenance mode from the available list and click the link to open the host details page.
4. Copy the Host ID from the Details section.
5. Go to Support API Explorer .
6. Locate and click the /hosts/{hostId}/commands/exitMaintenanceMode endpoint for HostsResource API to view the API parameters.
7. Click Try it out.
8. Enter the ID of your host in the hostId field.
9. Click Execute.
10. Verify that the maintenance mode status is cleared for the host by checking the Server response code.

    The operation is successful if the API response code is 200.

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

Cloudera bug: OPSAPS-65443 Phoenix requires Python 2.7

Phoenix requires Python 2.7 in order to run in Cloudera Manager 7.7.3 GA, CHF 1, and CHF 2.

Fix will be available in Cloudera Manager 7.7.3 CHF3.

OPSAPS-65104

Replication Manager does not work as expected when you upgrade from Cloudera Manager version 7.6.7 CHF2 to any Cloudera Manager version between 7.7.1 and 7.7.1 CHF13. If there were any Hive replication policies before the upgrade, Replication Manager does not respond after the upgrade.

If you are using Hive replication policies in Cloudera Manager 7.6.7 CHF2 or higher versions, you must only upgrade to Cloudera Manager 7.7.1 CHF14 version or higher.

OPSAPS-64385: Atlas's client.auth.enabled configuration is not configurable

In customer environments where user certifications are required to authenticate to services, the Apache Atlas UI constantly prompts for certs. By default, client.auth.enabled is set to TRUE. This causes Apache Atlas UI to show a popup to select a certificate.

Use an incognito window or a different browser that does not have certificate authentication enabled.

Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.7.3 release.

Cloudera Manager 7.7.3 Cumulative hotfix 5

Know more about the Cloudera Manager 7.7.3 cumulative hotfixes 5.

This cumulative hotfix was released on July 7, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF5 (version: 7.7.3-h4-42448625):
OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.3 CHF5 (version: 7.7.3-h4-42448625):

OPSAPS-59824: Set hive.hook.proto.base-directory for HMS by default

The hive.hook.proto.base-directory property, which is present for Hive on Tez (HiveServer2) was not available for the Hive metastore. Due to this, the HiveProtoEventsCleanerTask does not run and clean the old proto data.

This issue is now fixed and the hive.hook.proto.base-directory property is available in Cloudera Manager under Clusters HIVE-1 Configuration with a default value of /warehouse/tablespace/managed/hive/sys.db/query_data/.

OPSAPS-62805: Kafka role log file retrieval fails and diagnostic bundles do not contain the Kafka broker role logs

Fixed an issue where Kafka and Cruise Control role-level logs cannot be accessed due to a u'LOG4J2 issue. Added LOG4J2 in the log_search.py file to provide support to the LOG4J2 log type for accessing service logs through Cloudera Manager UI.

OPSAPS-65646: Upgraded Spring-security version

The Spring-security version is upgraded from 4.x.x. to 5.6.4 version to fix CVE issues.

OPSAPS-66435: Upgraded Woodstox version

The Woodstox version is upgraded to 6.4.0 version to fix CVE issues.

OPSAPS-65783: Impala Query Monitoring Status Check Alerts

TypeErrors appeared in Cloudera Manager Agent logs when viewing Impala query monitoring, which caused Impala Query Monitoring Status Check alerts in Cloudera Manager.

Fixed Python3 compatibility issue for Impala query monitoring in Cloudera Manager Agent.

The repositories for Cloudera Manager 7.7.3-CHF5 are listed in the following table:

Table 1: Cloudera Manager 7.7.3-CHF5

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/redhat7/yum/cloudera-manager.repo`

SLES 15	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/sles15/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h4-42448625/sles15/yum/cloudera-manager.repo`

Cloudera Manager 7.7.3 Cumulative hotfix 4

Know more about the Cloudera Manager 7.7.3 cumulative hotfixes 4.

This cumulative hotfix was released on May 18, 2023.

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

Platform Support Enhancements

- New OS Support
  - Cloudera Manager 7.7.3-CHF4 now supports SLES 15 SP4 for x86

Platform support for Cloudera Manager 7.7.3-CHF4

The following operating systems are supported when using Python 3.8 with the Cloudera Manager agents:

- RHEL 8.4
- RHEL 8.6
- RHEL 7.9

- SLES 15 SP4

Important:

- The supported Cloudera Manager's version for using SLES 15 SP4 is Cloudera Manager 7.7.3-CHF4
- The supported Cloudera Runtime version for using SLES 15 SP4 is CDP 7.1.8-CHF8
- Data Analytics Studio (DAS), NavEncrypt, and KTS are not supported in 7.1.8 when using SLES 15 SP4

Following known issues and their corresponding workarounds are shipped for Cloudera Manager 7.7.3 CHF4 (version: 7.7.3-h2-40943658):

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

OPSAPS-59723: Extra step required when using Cloudera Manager Trial installer on SLES 15 SP4

When using cloudera-manager-installer.bin to install a trial version of Cloudera Manager, the installation will fail.

Before running cloudera-manager-installer.bin, run the following command:

```
SUSEConnect --list-extensions
SUSEConnect -p sle-module-legacy/15.4/x86_64
zypper install libncurses5
```

OPSAPS-65243: Diagnostic data collection for YARN fails

Selecting Collect Diagnostic Data from the YARN Applications page fails to generate the diagnostic data.

None

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.3 CHF4 (version: 7.7.3-h2-40943658):

OPSAPS-67130: Log4J 1.2.17 replaced with Reload4J

In this release, Cloudera has replaced all Apache Log4j 1.2.x logging libraries included with Cloudera Manager 7.7.3 Cumulative hotfix 2 with equivalent Reload4j libraries.

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-65242: Alert Server Event cleanup issue

Fixed an issue where an Event Server cleanup did not work properly and now it works as intended, uses less CPU and keeps the events within the requested limits.

OPSAPS-65999: cert.py has Python 3 compatibility issues and an error occurs while performing any certificate generation and rotation operations

Fixed an issue in cert-manager code that decoded output from native OS commands. When Cloudera Manager attempts operations related to certificate generation or rotation, those operations may fail. Errors in the log file will indicate problems with string decoding. Running the cert-manager script directly from the CLI would also result in string decoding errors.

OPSAPS-66689: Hue logs get overwritten without a clear root cause

In previous implementations, multiple file handlers would write to a single log file, causing the Hue logs to be overwritten. Hue now uses a socket handler, which solves this problem.

OPSAPS-67080: Earlier, gathering Kudu diagnostic information within Cloudera Manager failed.

Now, gathering Kudu diagnostic information within Cloudera Manager no longer fails and works as expected..

The repositories for Cloudera Manager 7.7.3-CHF4 are listed in the following table:

Table 2: Cloudera Manager 7.7.3-CHF4

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/redhat7/yum/cloudera-manager.repo`

SLES 15	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/sles15/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h2-40943658/sles15/yum/cloudera-manager.repo`

Cloudera Manager 7.7.3 Cumulative hotfix 3

Know more about the Cloudera Manager 7.7.3 cumulative hotfixes 3.

This cumulative hotfix was released on May 09, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF3 (version: 7.7.3-h3-40765691):

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.3 CHF3 (version: 7.7.3-h3-40765691):

OPSAPS-65999: cert.py has Python 3 compatibility issues and an error occurs while performing any certificate generation and rotation operations

Fixed an issue in cert-manager code that decoded output from native OS commands. When Cloudera Manager attempts operations related to certificate generation or rotation, those operations may fail. Errors in the log file will indicate problems with string decoding. Running the cert-manager script directly from the CLI would also result in string decoding errors.

OPSAPS-67130: Log4J 1.2.17 replaced with Reload4J

In this release, Cloudera has replaced all Apache Log4j 1.2.x logging libraries included with Cloudera Manager 7.7.3 Cumulative hotfix 2 with equivalent Reload4j libraries.

The repositories for Cloudera Manager 7.7.3-CHF3 are listed in the following table:

Table 3: Cloudera Manager 7.7.3-CHF3

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h3-40765691/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h3-40765691/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h3-40765691/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.3-h3-40765691/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.7.3 Cumulative hotfix 2

Know more about the Cloudera Manager 7.7.3 cumulative hotfixes 2.

This cumulative hotfix was released on February 07, 2023.

Note:

1. Contact Cloudera Support for questions related to any specific hotfixes.
2. Cloudera recommends you to use Cloudera Manager 7.7.3-CHF2 with Cloudera Runtime 7.1.8-CHF3 as this includes a critical Apache Impala fix.

Following known issues and their corresponding workarounds are shipped for Cloudera Manager 7.7.3 CHF2 (version: 7.7.3-36823125):

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

OPSAPS-65706: ZooKeeper fails to restart after rollback

ZooKeeper server role fails to restart when you perform a rollback from Cloudera Manager 7.7.3 version to Cloudera Manager versions lower than 7.7.3.

The reason for ZooKeeper restart to fail is that post a rollback operation the previous version's ZooKeeper process starts and does not allow to start ZooKeeper process after rollback (as only 1 ZooKeeper process is allowed to stay running on the host).

> **Important:** This behavior is first seen with Zookeeper, however, the same problem applies to other roles on the host. After fixing Zookeeper role as mentioned in the below workaround, the following service role in the startup sequence also fails to start. In order to restart the cluster, apply the workaround to all roles on each host.

To restore the ZooKeeper server role to a running state, perform the below steps on all the hosts when the ZooKeeper server role fails to restart:

1. Run the following command to list the roles on the current host:

   ```
   sudo /opt/cloudera/cm-agent/bin/supervisorctl -c /run/cloude
   ra-scm-agent/supervisor/supervisord.conf status
   ```
2. Find the failing role in the above list, then run the following command to stop the role:

   ```
   sudo /opt/cloudera/cm-agent/bin/supervisorctl -c /run/cloude
   ra-scm-agent/supervisor/supervisord.conf
   supervisor> stop 123-zookeeper-server
   supervisor> remove 123-zookeeper-server
   supervisor> exit
   ```

   Replace the role id "123" with the appropriate number from the list in step 1.
3. Run the following command to terminate the Zookeeper processes by finding the PIDs:

   ```
   sudo ps -ef | grep -i zookeeper
   ```
4. Run the following command to remove the supervisor.conf of ZooKeeper from supervisor:

   ```
   rm /run/cloudera-scm-agent/supervisor/include/123-zookeeper-
   server.conf
   sudo kill -9 <PIDS obtained from the previous command>
   ```
5. Run the following command to refresh the configurations:

   ```
   sudo /opt/cloudera/cm-agent/bin/supervisorctl -c /run/cloude
   ra-scm-agent/supervisor/supervisord.conf reread
   ```
6. Start the ZooKeeper service from the Cloudera Manager UI.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.3 CHF2 (version: 7.7.3-36823125):

- OPSAPS-65578 - Fixed Cloudera Manager 7.7.3 dependency issue on Python 2
- OPSAPS-65557 - Fixed an issue where the Cloudera Manager agent fails to upgrade when you upgrade Cloudera Manager server from version 7.7.1 to 7.7.3.
- OPSAPS-65589 - Fixed an issue where the Cloudera Manager 7.7.3 is unable to start Apache Ranger and Apache Atlas services.
- OPSAPS-65443 - Fixed an issue where the Apache Phoenix service unable to start in Cloudera Data Platform (CDP) Private Cloud Base 7.1.8.

- OPSAPS-65623 - Fixed an issue where Cloudera Manager 7.7.3 unable to detect Python 3.8 from Redhat 7 Software Collections (SCL) repository.
- OPSAPS-64153 - Fixed an issue where the Core Settings service is getting added twice during cluster provisioning using a cluster template.
- OPSAPS-64614 - Fixed a Cloudera Manager upgrade issue, where the Cloudera Manager server fails to complete the upgrade and will not start, if a cluster had a legacy Core Configuration service with any number of Storage Operations roles.
- OPSAPS-65648 - Fixed an issue where the Data Analytics Studio, Query Processor, Key Trustee Server services unable to start without Python 2.

The repositories for Cloudera Manager 7.7.3-CHF2 are listed in the following table:

Table 4: Cloudera Manager 7.7.3-CHF2

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat7/yum/cloudera-manager.repo`

IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat8-ppc/yum`
IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-36823125/redhat7-ppc/yum`

Cloudera Manager 7.7.3 Cumulative hotfix 1

This Cloudera Manager 7.7.3 CHF1 lists the known issues that are affecting Cloudera Manager 7.7.3 and Cloudera Manager 7.7.3 CHF1 during installation or upgrade.

This cumulative hotfix was released on October 28, 2022.

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

Following known issues and their corresponding workarounds are shipped for Cloudera Manager 7.7.3 CHF1 (version: 7.7.3-33365545). For information about workarounds and long term resolutions, see KB article.

- OPSAPS-65578 - Cloudera Manager 7.7.3 dependency on Python 2

- OPSAPS-65557 - Cloudera Manager agent fails to upgrade when you upgrade Cloudera Manager server from version 7.7.1 to 7.7.3
- OPSAPS-65589 - Cloudera Manager 7.7.3 is unable to start Apache Ranger and Apache Atlas services
- OPSAPS-65443 - Apache Phoenix service does not start in Cloudera Data Platform (CDP) Private Cloud Base 7.1.8
- OPSAPS-65623 - Cloudera Manager 7.7.3 does not detect Python 3.8 from Redhat 7 Software Collections (SCL) repository
- OPSAPS-65648 - Data Analytics Studio, Query Processor, Key Trustee Server services do not start without Python 2

Additional Known issues related to Cloudera Manager 7.7.3 CHF1 (version: 7.7.3-33365545)

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

OPSAPS-64153: Core Settings service is getting added twice during cluster provisioning using a cluster template.

None.

OPSAPS-64614: Cloudera Manager server fails to complete the upgrade and will not start, if a cluster had a legacy Core Configuration service with any number of Storage Operations roles.

Cloudera Manager upgrade fails with the following error: ERROR MainThread:com.cloudera.server.cmf.Main: Server failed.java.lang.IllegalStateException: Revision was already prepared

Upgrading Cloudera Manager might fail if Cloudera Manager is running the Core Configuration service and is managing a compute cluster.

Before upgrading Cloudera Manager, you must remove any Storage Operations roles from the Core Configuration service as follows:

1. Log in to the Cloudera Manager server host.
2. Run the following command to stop the Cloudera Manager Server.

   ```
   sudo systemctl stop cloudera-scm-server
   ```

3. Open the CLI for the Cloudera Manager database using one of the following commands:
   - MySQL/MariaDB: mysql -u root -p
   - PostgreSQL: sudo -u postgres psql
   - Oracle: sqlplus system@localhost
4. Run the following SQL queries:
   a.
   ```
   select ROLE_ID from ROLES where ROLE_TYPE='STORAGEOPERATIONS';
   ```

   The query returns a set of ROLD_ID values. For each ROLE_ID, run the following SQL commands:

   ```
   delete from CONFIGS where ROLE_ID=<ROLE_ID>;
   delete from ROLE_STALENESS_STATUS where ROLE_ID=<ROLE_ID>;
   delete from ROLES where ROLE_TYPE='STORAGEOPERATIONS';
   ```

The repositories for Cloudera Manager 7.7.3-CHF1 are listed in the following table:

Table 5: Cloudera Manager 7.7.3-CHF1

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-33365545/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-33365545/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-33365545/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.3-33365545/redhat7/yum/cloudera-manager.repo`
	⚠ **Important:** You must use Cloudera Manager 7.7.3-CHF1 only when you need to use Python 3.8 for the Cloudera Manager agents. You must install Python 3.8 on all hosts before installing or upgrading to Cloudera Manager 7.7.3-CHF1. Cloudera Manager 7.7.3-CHF1 is only supported with RHEL 7.9, 8.4, and 8.6. For more information, see CDP Private Cloud Base Installation Guide.

Cloudera Manager 7.7.1 Release Notes

Known issues, fixed issues and new features for Cloudera Manager and CDP Private Cloud.

What's New in Cloudera Manager 7.7.1

New features and changed behavior for Cloudera Manager 7.7.1.

New features

Cloudera Manager High Availability

You can configure Cloudera Manager for high availability using an Active-Passive failover configuration by installing a load balancer and setting some additional configuration properties. See Configuring Cloudera Manager for High Availability.

Note: Cloudera Manager high availability feature is only supported with CDP Private Cloud Base 7.1.8 version or higher.

Cloudera Manager Secure Credential Store

You can configure Cloudera Manager to encrypt sensitive information stored in the Cloudera Manager database by configuring a Credential Storage Provider (CSP). See Configuring a Secure Credential Storage Provider for Cloudera Manager (Technical Preview) .

New Core Settings service replaces Core Configuration Service

The Core Settings Service allows you to store configuration data without needing to include HDFS in the cluster. See Core Settings Service.

Hive ACID replication policies using Replication Manager

You can create Hive ACID table replication policies in Replication Manager to copy ACID tables between CDP Private Cloud Base clusters for backup, load balancing, and other purposes. See Hive ACID table replication policies

Ozone replication policies using Cloudera Manager APIs

You can use Cloudera Manager APIs to create Ozone replication policies to replicate data in Ozone buckets between CDP Private Cloud Base 7.1.8 clusters or higher using Cloudera Manager 7.7.1 or higher. See Ozone replication policies.

Platform support updates

RedHat 8.6 is now a supported operating system

RedHat 8.6 is now supported with Cloudera Manager 7.7.1 and Cloudera Runtime 7.1.8.

MariaDB 10.6 is now a supported operating database

MariaDB 10.6 is now supported with Cloudera Manager 7.7.1 and Cloudera Runtime 7.1.8.

Updated PostgreSQL JDBC driver

The PostgreSQL JDBC driver bundled with Cloudera Manger is now updated to version 42.2.24.

Changed or updated features

Upgrades to Cloudera Manager 7.7.1 are not supported when there is a CDH 5 cluster present

Cloudera Manager will not allow an upgrade to CDP Private Cloud Base 7.1.8/Cloudera Manager 7.7.1 if Cloudera Manager is managing a CDH 5.x cluster. To upgrade a CDH 5 cluster:

1. Upgrade Cloudera Manager to version 6.3.4.
2. Upgrade CDH to version 6.3.4
3. Upgrade Cloudera Manager to version 7.6.5 or higher.

Functionality to disable Credential Storage Provider feature

Customers with Credential Storage Provider (CSP) enabled can disable the functionality if and when required.

New configuration parameters for user and group creation for Parcel file permissions

Decoupled the configuration setting in Cloudera Manager to allow user creation and updating file permissions to be performed separately during parcel installation. Two new configuration parameters have replaced the Create Users and Groups and Apply File Permissions for Parcels parameter. See Parcel Configuration Settings.

Optimize Avro metrics from agent to Service Monitor

Implemented an optimization in the communication between the Cloudera Manager Agent and Service Monitor that significantly increases monitoring throughput for services that rely on the affected part of the protocol. Examples of services that benefit from this improved scalability are Kudu and Kafka. No action is required to use the optimization.

Cloudera Manager now supports Active Directory objects with additional attributes

Cloudera Manager now supports Active Directory objects with additional attributes other than just accountExpires and objectClass for every new account creation. You can use these additional attributes of an object to identify or search for objects in the Active Directory network using LDAP queries.

You can now start using some of the sample attributes such as employeeType, Usertype, Manager, passwordNeverExpires, etc.

Fixed Issues in Cloudera Manager 7.7.1

Fixed issues in Cloudera Manager 7.7.1.

Cloudera Bug: OPSAPS-63605: Event Server index upgrade uses StringField for stack traces

Fixed an issue where the Event Server failed to start after a Cloudera Manager upgrade if the value of any event attribute (for example, content, stack trace) was longer than 32766 UTF-8 bytes.

Cloudera Bug: OPSAPS-63653: Validation on HDFS service to show Error if user selects wrong config to Enablegc Ranger plugin

An error will display if both RANGER and RANGER_AUTH_ENABLED configurations are enabled Only one should be enabled at a time.

Cloudera Bug: OPSAPS-63953: The authzmigrator authz_export.sh script hardcodes JAVA_HOME to /usr/java/default

The export script has been updated to fix this.

Cloudera Bug: OPSAPS-63992: Rolling restart unavailable for SRM

Initiating a rolling restart for the SRM service is now possible. Performing a rolling upgrade of the SRM service is now also possible.

Known Issues in Cloudera Manager 7.7.1

Known issues in Cloudera Manager 7.7.1

OPSAPS-65691: Cloudera Manager upgrade from 7.6.7 version fails with an ApiException error

While upgrading Cloudera Manager from Cloudera Manager 7.6.7 to Cloudera Manager 7.7.1, the upgrade failed with the following error message: ApiException: Expected boolean. Got END_OBJECT (error 400).

The following error is also logged in Cloudera Manager server log: scm-web-198:com.cloudera.server.web.cmf.home.SystemHealth: HealthInfo Exception:Exception occurred inside setter of com.cloudera.cmf.model.DbProcess.specialFileInfoForDb

Upgrade to the Cloudera Manager 7.7.1 CHF5 or later versions where this issue is fixed.

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
    - Name = hadoop.security.group.mapping.ldap.bind.password
    - Value = (Enter the LDAP bind password here)
    - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

OPSAPS-62805: Kafka role log file retrieval fails and diagnostic bundles do not contain the Kafka broker role logs.

Kafka and Cruise Control role-level logs cannot be accessed due to a u'LOG4J2 issue.

None

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_namenode_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-65213: Ending the maintenance mode for a commissioned host with either an Ozone DataNode role or a Kafka Broker role running on it, might result in an error.

You may see the following error if you end the maintenance mode for Ozone and Kafka services from Cloudera Manager when the roles are not decommissioned on the host.

```
Execute command Recommission and Start on service OZONE-1
Failed to execute command Recommission and Start on service OZ
ONE-1
Recommission and Start
Command Recommission and Start is not currently available for e
xecution.
```

To resolve this issue, use the API support feature to take the host out of maintenance mode.

1. Log into Cloudera Manager as an Administrator.
2. Go to Hosts All Hosts .
3. Select the host for which you need to end the maintenance mode from the available list and click the link to open the host details page.
4. Copy the Host ID from the Details section.
5. Go to Support API Explorer .
6. Locate and click the /hosts/{hostId}/commands/exitMaintenanceMode endpoint for HostsResource API to view the API parameters.
7. Click Try it out.
8. Enter the ID of your host in the hostId field.
9. Click Execute.
10. Verify that the maintenance mode status is cleared for the host by checking the Server response code.

    The operation is successful if the API response code is 200.

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

OPSAPS-64029

When Cloudera Manager is upgraded from prior versions to 7.7.1 or later, Queue Manager (QM) will be flagged as stale due to new support for auto-configuration of QM with Yarn Resource Manager (RM).

Restart the QM role at a convenient time.

OPSAPS-63881: When CDP Private Cloud Base is running on RHEL/CentOS/Oracle Linux 8.4, services fail to start because service directories under the /var/lib directory are created with 700 permission instead of 755.

Run the following command on all managed hosts to change the permissions to 755. Run the command for each directory under /var/lib:

```
chmod -R 755 [***PATH_TO_SERVICE_DIR***]
x
```

OPSAPS-63838: Cloudera Manager is unavailable after failover

When high availability is enabled for Cloudera Manager, and there is a failover from the Active to the Passive server, the Cloudera Manager server may be unavailable for 15-20 seconds when failing back to the Active server.

Known Issues in Replication Manager

OPSAPS-64388 - Schedule creation API doesn't stop user from creating a bucket within a bucket

When the bucket path in the source and target clusters are different, the replication policy creation API does not fail but the Ozone replication fails with the **Ozone File Listing Command Failed** error.

Before you create the Ozone replication policy using Cloudera Manager APIs, ensure that the path of the bucket which includes the volume name and bucket name in the target cluster is same as in the source cluster.

OPSAPS-64466 - JCKS way of authentication on Ozone causes YARN to go down on Auto-TLS cluster

During the Ozone replication policy job for OBS buckets, the YARN application goes down and does not restart when the authentication credentials for Auto-TLS is provided using the hadoop.security.credential.provider.path property where the value is the JKS file.

Configure fs.s3a.secret.key and fs.s3a.access.key in the Ozone Client Advanced Configuration Snippet (Safety Valve) property in the ozone-conf.xml and ozone-site.xml files so that the Ozone replication policies use the authentication credentials in these files for OBS bucket replication.

OPSAPS-64501 - Hive 3 replication | CMHA | Failover doesn't go to completion status on its own

This behavior is observed when high availability is enabled for both source and target clusters' Cloudera Manager instances.

When you click Actions Start Failover for a successful Hive ACID table replication policy on the **Replication Policies** page, the policy job does not transition to failover status for a long time. When you click Actions Revert/Complete failover for the same replication policy, the policy transitions to failover complete and then eventually disables the policy.

OPSAPS-64879 - Replication policies with empty name are not shown on the UI

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

Provide a unique replication policy name during replication policy creation.

OPSAPS-65104

Replication Manager does not work as expected when you upgrade from Cloudera Manager version 7.6.7 CHF2 to any Cloudera Manager version between 7.7.1 and 7.7.1 CHF13. If there were any Hive replication policies before the upgrade, Replication Manager does not respond after the upgrade.

If you are using Hive replication policies in Cloudera Manager 7.6.7 CHF2 or higher versions, you must only upgrade to Cloudera Manager 7.7.1 CHF14 version or higher.

Log4j-1x remediation

CDP Private Cloud Base 7.1.7 SP1 and CDP Private Cloud Base 7.1.8 uses Reload4j and does not contain those CVEs but the files were renamed to log4j-1.2.17-cloudera6.jar. This still sets off scanners, but retained the log4j prefix that made for an easy transition for dependencies. In CDP Private Cloud Base 7.1.7 SP2, the log4j-1.2.17-cloudera6.jar files were renamed to reload4j-1.2.22.jar in the CDP parcel and should not set off scanners.

These remaining JARs are related to Cloudera Manager and are in 7.7.1 but 7.6.7 has them removed:

/opt/cloudera/parcels/CDH-7.1.8-1.cdh7.1.8.p0.30990532/jars/log4j-1.2.17-cloudera6.jar

/opt/cloudera/cm/cloudera-navigator-audit-server/log4j-1.2.17-cloudera6.jar

/opt/cloudera/cm/cloudera-navigator-server/jars/log4j-1.2.17-cloudera6.jar

/opt/cloudera/cm/cloudera-scm-telepub/jars/log4j-1.2.17-cloudera6.jar

/opt/cloudera/cm/common_jars/log4j-1.2.17-cloudera6.5e6c49dac2e98e54fc9a8438826fa763.jar

/opt/cloudera/cm/lib/log4j-1.2.17-cloudera6.jar

Workaround: To get every log4j-1x version replaced with ones named reload4j, you must be on CDP Private Cloud Base 7.1.8 latest Cumulative hotfixes or CDP Private Cloud Base 7.1.9 and associated Cloudera Manager versions. (CDP Private Cloud Base 7.1.7 SP1 uses reload4j but the name still says log4j).

Note: The presence of log4j-1.2-api-2.17.1.jar and log4j-1.2-api-2.18.0.jar does not mean log4j1 is present. log4j-1.2-api does not contain any vulnerable code which can be seen from the Maven page where no CVEs are listed, either directly or through indirect dependencies.

Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.7.1 release.

Cloudera Manager 7.7.1 Cumulative hotfix 23

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 23 (version: 7.7.1-h32-56750899).

This cumulative hotfix was released on August 29, 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 7.7.1 CHF23 (version: 7.7.1-h32-56750899):

OPSAPS-71005: Remote command work is using a single-threaded executor

By default, Replication Manager runs the remote commands for a replication policy through a single-thread executor. Now, 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.

The repositories for Cloudera Manager 7.7.1-CHF23 are listed in the following table:

Table 6: Cloudera Manager 7.7.1-CHF23

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h32-56750899/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 22

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 22 (version: 7.7.1-h31-55950782).

This cumulative hotfix was released on August 2, 2024.

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

New features and changed behavior for Cloudera Manager 7.7.1 CHF22 (version: 7.7.1-h31-55950782): Custom properties atlas.jaas.KafkaClient.option.password was available in a clear text format in CDP cluster services when Kerberos authentication was not present.

To provide a secured access, two new fields are introduced for username / password and a radio field for loginModule for Kerberos or Plain selection.

atlas.jaas.KafkaClient.option.username=username

atlas.jaas.KafkaClient.option.password=<password is in clear text>

atlas.jaas.KafkaClient.option.loginModuleName=KERBEROS(default)

Platform Support Enhancements

New JDK Version: Azul Open JDK 8 and Azul Open JDK 11 are supported with Cloudera Manager 7.7.1 CHF22 and higher versions.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF22 (version: 7.7.1-h31-55950782):

OPSAPS-68752: Snapshot-diff delta is incorrectly renamed/deleted twice during on-premises to cloud replication

The snapshots created during replication are deleted twice instead of once, which results in incorrect snapshot information. This issue is fixed. For more information, see Cloudera Customer Advisory 2023-715: Replication Manager may delete its snapshot information when migrating from on-prem to cloud.

OPSAPS-60139: Staleness performance issue in clusters with a large number of roles

In large clusters, Cloudera Manager takes a long time to display the Configuration Staleness icon after a service configuration change. This issue is fixed now by improving the performance of the staleness-checking algorithm.

OPSAPS-60331: Active Directory creates invalid Service Principal Names(SPN) when generating Kerberos credentials

If Cloudera Manager is configured to use Active Directory as a Kerberos KDC, and is also configured to use /etc/cloudera-scm-server/cmf.keytab as the KDC admin credentials, you should no longer encounter errors when generating Kerberos credentials.

OPSAPS-67068: Updating interval value used by Ranger service for creating ranger_audits collection in Solr

Updated ranger.audit.solr.time.interval to 60000 ms.

OPSAPS-66924: HBase snapshot export deletes target folder in case of failure

HBase snapshot export no longer deletes the target folder if the snapshot export fails during HBase replication using Replication Manager.

OPSAPS-65913: Unstable config generation of Hue with multiple HS2 servers

Fixed an issue of unstable config generation of Hue when more than 1 HS2 servers are present without a configured load-balancer.

OPSAPS-66050: Hive performance issues when hive.auto.convert.join.noconditionaltask.size property was set to a low value

The hive.auto.convert.join.noconditionaltask.size property was set to a low value of 50 MB. This resulted in performance issues when the size of the container is 2 GB or more and if the sum of size of the tables/partitions is more than 50 MB.

This issue is now fixed and the default value for hive.auto.convert.join.noconditionaltask.size is set to 256 MB.

OPSAPS-70689: Enhanced performance of DistCp CRC check operation

When a MapReduce job for an HDFS replication policy job fails, or when there are target-side changes during a replication job, Replication Manager initiates the bootstrap replication process. During this process, a cyclic redundancy check (CRC) check is performed by default to determine whether a file can be skipped for replication.

By default, the CRC for each file is queried by the mapper (running on the target cluster) from the source cluster's NameNode. The round trip between the source and target cluster for each file consumes network resources and raises the cost of execution. To improve the performance, you can set the following variables to true, on the target cluster, to improve the performance of the CRC check for the Cloudera Manager Clusters *HDFS SERVICE* Configuration HDFS_REPLICATION_ENV_SAFETY_VALVE property:

- ENABLE_FILESTATUS_EXTENSIONS
- ENABLE_FILESTATUS_CRC_EXTENSIONS

By default, these are set to false.

After you set the key-value pairs, the CRC for each file is queried locally from the NameNode on the source cluster and copied over to the target cluster at the end of the replication process, which reduces the cost because round trip is between two nodes of the same cluster. The CRC checksums are written to the file listing files.

OPSAPS-70685: Post Copy Reconciliation (PCR) for HDFS replication policies between on-premises clusters

To add the Post Copy Reconciliation (PCR) script to run as a command step during the HDFS replication policy job run, you can enter the SCHEDULES_WITH_ADDITIONAL_DEBUG_STEPS = [***ENTER COMMA-SEPARATED LIST OF NUMERICAL IDS OF THE REPLICATION POLICIES***] key-value pair in the target Cloudera Manager Clusters *HDFS SERVICE* hdfs_replication_env_safety_valve property.

To run the PCR script on the HDFS replication policy, use the `/clusters/[***CLUSTER NAME***]>/services/[***SERVICE***]/replications/[***SCHEDULE ID***]/postCopyReconciliation` API.

For more information about the PCR script, see How to use the post copy reconciliation script for HDFS replication policies.

The repositories for Cloudera Manager 7.7.1-CHF22 are listed in the following table:

Table 7: Cloudera Manager 7.7.1-CHF22

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h31-55950782/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 21

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 21 (version: 7.7.1-h29-53489657).

This cumulative hotfix was released on May 28, 2024.

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

Following are the list of known issues that were shipped for Cloudera Manager 7.7.1 CHF21 (version: 7.7.1-h29-53489657):

OPSAPS-71067: Wrong interval sent from the Replication Manager UI after Ozone replication policy submit or edit process.

When you edit the existing Ozone replication policies, the schedule frequency changes unexpectedly.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF21 (version: 7.7.1-h29-53489657):

OPSAPS-69018: Cloudera Manager fails to support multiple SAML role values

When multiple values for the SAML role assignment attribute are returned in an assertion, Cloudera Manager only reads the first attribute value returned in an assertion list.

Since the attribute typically reflects a user's LDAP groups, multiple values are common and can include any number of values which may or may not be mapped to roles in Cloudera Manager, in any order. This can cause authorization failures, or unexpected limited access rights in Cloudera Manager. This issue is fixed now.

OPSAPS-68418: Partition missing during column statistics import operation

A data-race issue found during the Hive metadata export step during the Hive external table replication policy run has been fixed so that concurrent modifications made to the partitions during the export operation does not result in import failure.

OPSAPS-70422: Metadata replication by Hive external table replication policies can use the username specified in the "Run as username(on source)" field.

The USE_PROXY_USER_FOR_CLOUD_TRANSFER=true key-value pair for the target Cloudera Manager Clusters Hive service Configuration Hive Replication Environment Advanced Configuration Snippet (Safety Valve) property ensures that the metadata transfer step during the Hive external table replication process does not ignore the username specified in the Run as username (on source) field. You can add the required username in the Run as username (on source) field when you create the Hive external table replication policy in Replication Manager.

Note: Add the USE_PROXY_USER_FOR_CLOUD_TRANSFER=true on the source cluster when you want to replicate Hive data to CDP Public Cloud.

The repositories for Cloudera Manager 7.7.1-CHF21 are listed in the following table:

Table 8: Cloudera Manager 7.7.1-CHF21

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h29-53489657/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 20

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 20 (version: 7.7.1-h28-52058805).

This cumulative hotfix was released on April 17, 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 7.7.1 CHF20 (version: 7.7.1-h28-52058805):

OPSAPS-65460: The current RetryWrapper implementation does not work as expected when the transient database error appears

Hive replication policies no longer fail with the "javax.persistence.OptimisticLockException" error on the source cluster during the Hive export step.

The repositories for Cloudera Manager 7.7.1-CHF20 are listed in the following table:

Table 9: Cloudera Manager 7.7.1-CHF20

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h28-52058805/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 19

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 19 (version: 7.7.1-h26-51507507).

This cumulative hotfix was released on March 22, 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 7.7.1 CHF19 (version: 7.7.1-h26-51507507):

OPSAPS-69609: Custom properties atlas.jaas.KafkaClient.option.password appears in a clear text in CDP cluster services.

CDP Private Cloud Base 7.1.8 cluster had a configuration property with a clear text password which is a information security breach. The password is now masked or encrypted in the cluster.

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.

The repositories for Cloudera Manager 7.7.1-CHF19 are listed in the following table:

Table 10: Cloudera Manager 7.7.1-CHF19

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h26-51507507/ubuntu1804/apt/cloudera-manager.list`

Technical Service Bulletins

TSB 2024-734: The Replication Policies page of Replication Manager is non-functional in Cloudera Manager UI

For the latest update on this issue see the corresponding Knowledge article: TSB 2024-734: The Replication Policies page of Replication Manager is non-functional in Cloudera Manager UI

Cloudera Manager 7.7.1 Cumulative hotfix 18

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 18 (version: 7.7.1-h23-49934043).

This cumulative hotfix was released on February 9, 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 7.7.1 CHF18 (version: 7.7.1-h23-49934043):

OPSAPS-69207: Customizable authorization-migration-site.xml for Sentry-to-Ranger migration

During the Hive external table replication creation process, you can modify the properties in the authorization-migration-site.xml file on the **Sentry-Ranger Migration** tab. This tab appears after you choose the If Sentry permissions were exported from the CDH cluster, import both Hive object and URL permissions or If Sentry permissions were exported from the CDH cluster, import only Hive object permissions option in the Hive external table replication policy wizard General Permissions field.

The repositories for Cloudera Manager 7.7.1-CHF18 are listed in the following table:

Table 11: Cloudera Manager 7.7.1-CHF18

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/ubuntu1804/apt/cloudera-manager.list`

IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat7-ppc/yum`
IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h23-49934043/redhat8-ppc/yum`

Cloudera Manager 7.7.1 Cumulative hotfix 17

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 17.

This cumulative hotfix was released on January 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 7.7.1 CHF17 (version: 7.7.1-h20-49154526):

OPSAPS-69411

Users will now be able to export sentry data only for given Hive objects (databases and tables and the respective URLs) by using the config "authorization.migration.export.migration_objects" during export.

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-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

To fix this issue, perform the instructions from the Emitting the LDAP Bind password in core-site.xml for client configurations section to emit the LDAP Bind password in core-site.xml for client configurations.

OPSAPS-69057: Customizable authorization-migration-site.xml for Sentry-to-Ranger migration

You can now add additional arguments to override any existing property in the authorization-migration-site.xml file. The Sentry to Ranger migration process during the Hive replication policy run uses this file. These additional arguments are used during the Sentry to Ranger migration process for Sentry export on the source and Ranger import on the destination. You can enter the arguments using the CM API body as shown in the following sample snippet:

```
“hiveArguments”: {
    ...
    “rangerImportProperties”: {
         “authorization.migration.destination.location.prefix”: “
hdfs://nameservice”,
         “some.other.prop”: “some_property”
     },
     “sentryExportProperties”: {
          “authorization.migration.role.permissions”: “true”,
          “export.prop”: “export_prop_sentry”,
          “authorization.migration.destination.location.prefix”:
“hdfs://nameservice”
      },
  ...
}
```

The repositories for Cloudera Manager 7.7.1-CHF17 are listed in the following table:

Table 12: Cloudera Manager 7.7.1-CHF17

Repository Type	Repository Location
RHEL 8 Compatible	Repository: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat8/yum Repository File: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat8/yum/cloudera-manager.repo
RHEL 7 Compatible	Repository: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat7/yum Repository File: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat7/yum/cloudera-manager.repo
SLES 12	Repository: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/sles12/yum Repository File: https://*USERNAME*:*PASSWORD*@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/sles12/yum/cloudera-manager.repo

Repository Type	Repository Location

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/ubuntu1804/apt/cloudera-manager.list`

IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat7-ppc/yum`
IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/7.7.1-h20-49154526/redhat8-ppc/yum`

Technical Service Bulletins

TSB 2024-734: The Replication Policies page of Replication Manager is non-functional in Cloudera Manager UI

Cloudera discovered that certain versions of Cloudera Manager have a non-functional **Replication Policies** page. On the affected versions, visiting the page in Cloudera Manager results in a User Interface (UI) error and the page will not load. Because of this error, creating new replication policies, editing or deleting existing policies and viewing the existing policies on the UI is not possible.

Pre-existing policies will continue to run scheduled as expected. The execution of policies and the REST API of Cloudera Manager are not affected by this issue.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: TSB 2024-734: The Replication Policies page of Replication Manager is non-functional in Cloudera Manager UI

Cloudera Manager 7.7.1 Cumulative hotfix 16

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 16.

This cumulative hotfix was released on November 3, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF16 (version: 7.7.1-h17-46671550):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF16 (version: 7.7.1-h17-46671550):

OPSAPS-68422: Incorrect HBase shutdown command can lead to inconsistencies

Cloudera Manager uses an incomplete stop command when you stop the HBase service or the corresponding roles on a 7.1.8 or higher private cloud cluster. Due to this, the Cloudera Manager cannot gracefully stop the processes and kill them after a set timeout. This could lead to metadata corruption.

This issue is fixed now.

The repositories for Cloudera Manager 7.7.1-CHF16 are listed in the following table:

Table 13: Cloudera Manager 7.7.1-CHF16

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/ubuntu1804/apt/cloudera-manager.list`

IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat7-ppc/yum`
IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h17-46671550/redhat8-ppc/yum`

Cloudera Manager 7.7.1 Cumulative hotfix 15

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 15.

This cumulative hotfix was released on October 2, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF15 (version: 7.7.1-h16-45582990):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF15 (version: 7.7.1-h16-45582990):

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

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. This column now displays the correct message.

OPSAPS-67888

The ‘Hive-On-Tez Replication Metrics Getter’ command did not reschedule when the Hive-on-Tez service became unavailable. The command now reschedules automatically when the Hive-on-Tez service is unavailable and also displays a message on the Cloudera Manager UI.

OPSAPS-68387

The **Status** column on the Cloudera Manager Replication Replication Policies page was incorrectly showing **Skipped** for Hive ACID replication policy jobs when the job status was unknown. The column now shows the **Waiting for Update** status for the Hive ACID replication policy jobs until the job status is confirmed.

OPSAPS-68494

Replication Metric getter failed when the hive.resultset.use.unique.column.names parameter was set to false because the resulting columns were non-unique. The Replication Metric getter now configures the hive.resultset.use.unique.column.names parameter to true during its JDBC session to override the service configuration.

The repositories for Cloudera Manager 7.7.1-CHF15 are listed in the following table:

Table 14: Cloudera Manager 7.7.1-CHF15

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h16-45582990/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 14

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 14.

This cumulative hotfix was released on September 7, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF14 (version: 7.7.1-h14-44760873):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

CDPD-75871: Hive external table replication fails after you upgrade from 7.7.1 CHF14

After you upgrade, the Hive external table replication policies fail during the “Hive import” step if the following conditions are true:

- The default setting columnStatsImportMultiThreaded = true in the Cloudera Manager Clusters *HIVE SERVICE* Configuration hive_replication_env_safety_valve property is retained after the upgrade process.
- You are using HA Hive Metastore, and are using Hive and Impala to query source tables.

Perform the following steps to resolve the issue:

1. Go to the target Cloudera Manager Clusters *HIVE SERVICE* Configuration tab.
2. Locate the hive_replication_env_safety_valve property.
3. Add COLUMN_STATS_IMPORT_MULTI_THREADED=false, and Save the changes.
4. Restart the Hive service.
5. Run the Hive external table replication policy.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF14 (version: 7.7.1-h14-44760873):

OPSAPS-67641

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-65104: Importing table column statistics for Hive replication is thread-safe but causes performance regression.

To resolve this issue, perform the following steps:

1. Go to the Cloudera Manager Clusters *HIVE SERVICE* Configuration tab.
2. Locate the **hive_replication_env_safety_valve** property.
3. Add only *one* of the following key-value pair depending on your requirement:

    - COLUMN_STATS_IMPORT_MULTI_THREADED=true

      This ensures that the column statistics import operation is multi-threaded for Hive replication.
    - SKIP_COLUMN_STATS_IMPORT=true

      This ensures that the column statistics import is skipped entirely.

The repositories for Cloudera Manager 7.7.1-CHF14 are listed in the following table:

Table 15: Cloudera Manager 7.7.1-CHF14

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h14-44760873/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 13

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 13.

This cumulative hotfix was released on August 18, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF13 (version: 7.7.1-h13-44113658):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
    - Name = hadoop.security.group.mapping.ldap.bind.password
    - Value = (Enter the LDAP bind password here)
    - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF13 (version: 7.7.1-h13-44113658):

OPSAPS-67942: Installation failed due to schematool error

Setting the hive.hook.proto.base-directory for Hive Metastore (HMS) in hive-site.xml is causing sys.db creation to fail because of incompatibility issues between Cloudera Manager 7.7.1 and CDH 7.1.7 SP1/SP2. This patch addresses the issue and sets the above configuration only if the CDH version of Hive is at least CDH 7.1.8.

OPSAPS-67897, OPSAPS-68023

Ozone replication policies do not fail and the files on the target cluster are deleted successfully when you set the Advanced Options Delete Policy option to 'Delete to Trash' or 'Delete Permanently' (using Replication Manager) or if you set the `removeMissingFiles` parameter to 'True' (using Cloudera Manager REST APIs) during the Ozone replication policy creation process.

The repositories for Cloudera Manager 7.7.1-CHF13 are listed in the following table:

Table 16: Cloudera Manager 7.7.1-CHF13

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h13-44113658/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 12

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 12.

This cumulative hotfix was released on July 28, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF12 (version: 7.7.1-h12-43414392):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF12 (version: 7.7.1-h12-43414392):

OPSAPS-64882: Upgraded PostgreSQL version

The PostgreSQL version is upgraded from 42.2.24.jre7 to 42.5.1 version to fix CVE issues.

OPSAPS-65831: DistCp job deletes multiple threads for bootstrap replication

Performance of bootstrap or FFL (full file listing) replication for destination-side delete of paths missing from the source is improved with the following optional behaviors.

- FFL replication schedules all the missing paths for deletion regardless of parent relationships. When the `com.cloudera.enterprise.distcp.parent-only-delete.enabled` safety valve is set to "true", only the topmost deleted paths are scheduled for deletions and their descendants or children cannot be accessed. This is optional and by default turned off (which preserves the previous behavior).
- Delete requests can be issued from multiple threads concurrently to improve performance, and can be enabled and configured using the following safety valves:
  - `com.cloudera.enterprise.distcp.parallel-ffl-delete.enabled`. Default is "false".
  - `com.cloudera.enterprise.distcp.parallel-ffl-delete.threads`. Default is 20.
  - `com.cloudera.enterprise.distcp.parallel-ffl-delete.max-queue-size`. Default is 10000.

The repositories for Cloudera Manager 7.7.1-CHF12 are listed in the following table:

Table 17: Cloudera Manager 7.7.1-CHF12

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/sles12/yum/cloudera-manager.repo`

Repository Type	Repository Location

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h12-43414392/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 11

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 11.

This cumulative hotfix was released on July 4, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF11 (version: 7.7.1-h11-42449156):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF11 (version: 7.7.1-h11-42449156):

OPSAPS-67490: Cloudera Manager unable to deploy the Hadoop User Group Mapping LDAP Bind User Password configuration completely

Fixed an issue where Cloudera Manager is unable to deploy complete configurations from Core Configurations (CORE_SETTINGS-1) to client configurations under local /etc directory in the JCEKS file.

The repositories for Cloudera Manager 7.7.1-CHF11 are listed in the following table:

Table 18: Cloudera Manager 7.7.1-CHF11

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h11-42449156/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 10

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 10.

This cumulative hotfix was released on June 20, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF10 (version: 7.7.1-h10-41966254):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.

3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF10 (version: 7.7.1-h10-41966254):

OPSAPS-65646: Upgraded Spring-security version

The Spring-security version is upgraded from 4.x.x. to 5.6.4 version to fix CVE issues.

OPSAPS-66435: Upgraded Woodstox version

The Woodstox version is upgraded to 6.4.0 version to fix CVE issues.

OPSAPS-67463

After you edited a replication policy in Replication Manager, the schedule always reset to ‘Immediate’ which is incorrect. This issue is fixed.

OPSAPS-66517: Changing password from Home username Change Password bypasses validation

In Cloudera Manager, while changing the password for the current user from Home username Change Password , password validations are completely bypassed. This issue is fixed now and it now validates the password before saving the new password.

The repositories for Cloudera Manager 7.7.1-CHF10 are listed in the following table:

Table 19: Cloudera Manager 7.7.1-CHF10

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h10-41966254/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 9

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 9.

This cumulative hotfix was released on May 18, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF9 (version: 7.7.1-h9-40960082):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF9 (version: 7.7.1-h9-40960082):

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_namenode_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. This issue is fixed now.

OPSAPS-59824: Set hive.hook.proto.base-directory for HMS by default

The hive.hook.proto.base-directory property, which is present for Hive on Tez (HiveServer2) was not available for the Hive metastore. Due to this, the HiveProtoEventsCleanerTask does not run and clean the old proto data.

This issue is now fixed and the hive.hook.proto.base-directory property is available in Cloudera Manager under Clusters HIVE-1 Configuration with a default value of /warehouse/tablespace/managed/hive/sys.db/query_data/.

The repositories for Cloudera Manager 7.7.1-CHF9 are listed in the following table:

Table 20: Cloudera Manager 7.7.1-CHF9

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/sles12/yum/cloudera-manager.repo`

Repository Type	Repository Location

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h9-40960082/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 8

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 8.

This cumulative hotfix was released on May 04, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF8 (version: 7.7.1-h8-40487303):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF8 (version: 7.7.1-h8-40487303):

OPSAPS-66689: Hue logs get overwritten without a clear root cause

In previous implementations, multiple file handlers would write to a single log file, causing the Hue logs to be overwritten. Hue now uses a socket handler, which solves this problem.

The repositories for Cloudera Manager 7.7.1-CHF8 are listed in the following table:

Table 21: Cloudera Manager 7.7.1-CHF8

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h8-40487303/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 7

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 7.

This cumulative hotfix was released on April 20, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF7 (version: 7.7.1-h7-39964696):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.

3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF7 (version: 7.7.1-h7-39964696):

- **OPSAPS-64429-Failure on template import if StubDFS created before CORE_SETTINGS**

  If the service of type CORE_SETTINGS was explicitly defined in a cluster template, you could run into a failure to import such template. This issue is fixed now.
- **OPSAPS-64526**

  When Cloudera Manager is configured to use PAM as an external authentication provider (for logins to Cloudera Manager), if a valid username is denied due to password expiration, then Cloudera Manager will deny all future login attempts for any username. This issue is fixed now.
- **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.
- **NAV-7341-Spark extractor issues with HDFS namespace**

  When Navigator is installed and started with CDP installation, the Agent could move Spark lineage files out of the lineage directory which are not processed by Navigator. This issue is fixed now.

- The repositories for Cloudera Manager 7.7.1-CHF7 are listed in the following table:

Table 22: Cloudera Manager 7.7.1-CHF7

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h7-39964696/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 6

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 6.

This cumulative hotfix was released on April 13, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF6 (version: 7.7.1-h4-39235984):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixes that were shipped for Cloudera Manager 7.7.1 CHF6 (version: 7.7.1-h4-39235984):

- **OPSAPS-63558**

  Previously, DistCp did not correctly report renames and deletes in case of snapshot diff-based HDFS replications. This change extends DistCp's output report to contain counters related to snapshot diff-based replications beside the already reported counters. These counters are added to the following group: com.cloudera.enterprise.distcp.DistCpSyncCounter.

  The following new counters are added:

  - FILES_MOVED_TO_COMMON_TEMP_DIR: Number of files and directories moved to a common temporary directory to be renamed or deleted later in the process. This counter is the sum of FILES_DELETED_VIA_COMMON_TEMP_DIR and FILES_RENAMED_VIA_COMMON_TEMP_DIR.
  - FILES_DELETED_VIA_COMMON_TEMP_DIR: Number of files moved to a common temporary directory to be deleted later.
  - FILES_RENAMED_VIA_COMMON_TEMP_DIR: Number of files moved to a common temporary directory first, then moved to their final place.
  - FILES_DIRECT_DELETED: Number of files deleted directly. This is a feature introduced in OPSAPS-63759.
  - FILES_DIRECT_RENAMED: Number of files renamed directly, without moving to an intermediate temporary directory. This is a feature introduced in OPSAPS-63930.
  - FILES_DIRECT_RENAMED_VIA_TEMP_LOCATION: Number of files moved to an intermediate temporary directory and then renamed. This intermediate temporary directory is different from the common temporary directory referenced in the FILES_RENAMED_VIA_COMMON_TEMP_DIR counter's description. This is also related to OPSAPS-63930.

  The common temporary directory is a sibling of the replication target directory.

  The values of FILES_DELETED_VIA_COMMON_TEMP_DIR and FILES_DIRECT_DELETED are also aggregated in the replication result as the number of files deleted.
- **OPSAPS-65131**

  When you enter incorrect volume or bucket details in an Ozone replication policy, an error appears and you are logged out of Cloudera Manager. This issue is fixed.

  When you enter incorrect volume or bucket details, an error appears and you are not logged out of Cloudera Manager.
- **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-66107**

  Avoiding unnecessary Resource Manager scheduled refresh in Global Pools Refresh command. During Autoscaling in the public cloud, the scheduled Global Pools refresh command was causing conflicts with the Resource Manager refresh command that is triggered by commission and decommission commands of Yarn service (which caused Autoscale failures as the Resource Manager refresh command was not available). This issue is fixed now.

- The repositories for Cloudera Manager 7.7.1-CHF6 are listed in the following table:

Table 23: Cloudera Manager 7.7.1-CHF6

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/ubuntu1804/apt/cloudera-manager.list`

IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat8-ppc/yum`
IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h4-39235984/redhat7-ppc/yum`

Cloudera Manager 7.7.1 Cumulative hotfix 5

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 5.

This cumulative hotfix was released on March 14, 2023.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF5 (version: 7.7.1-h2-38419853):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixes that were shipped for Cloudera Manager 7.7.1 CHF5 (version: 7.7.1-h2-38419853):

- **OPSAPS-61474: Knox token API call failed with a 404 error while fetching the Knox token using token API in the Knox homepage topology**

  Fixed an issue where Knox's data/applications folder gets recreated every time when Knox service starts.
- **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-59363: TLS 1.0 and 1.1 protocols are out-of-date and contain security vulnerabilities**

  This issue has been fixed by disabling the old TLS (1.0 and 1.1) protocols for every JVM started by Cloudera Manager and upgrading to a higher version of the protocol (1.2 or 1.3). Cloudera Manager now only supports TLS 1.2 for Java 8. For Java 11 and higher versions, Cloudera Manager supports TLS 1.2 and TLS 1.3.

The repositories for Cloudera Manager 7.7.1-CHF5 are listed in the following table:

Table 24: Cloudera Manager 7.7.1-CHF5

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-h2-38419853/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 4

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 4.

This cumulative hotfix was released on February 23, 2023.

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

Following are the Common Vulnerabilities and Exposures (CVE)'s that are fixed in the Cloudera Manager 7.7.1 CHF4 (version: 7.7.1-38008529) release:

- CVE-2022-41966

Following known issues and their corresponding workarounds are shipped for Cloudera Manager 7.7.1 CHF4 (version: 7.7.1-38008529):

- **OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations**

  If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

  This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

  Set the LDAP Bind password through the HDFS client configuration safety valve.

  1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
  2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
  3. Add an entry with the following values:
     - Name = hadoop.security.group.mapping.ldap.bind.password
     - Value = (Enter the LDAP bind password here)
     - Description = Password for LDAP bind account
  4. Then click the Save Changes button to save the safety valve entry.
  5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

CDPD-49716

Unable to access the Hue UI on a Knox-enabled cluster.

Before you access the Hue UI on a Knox-enabled cluster, ensure that you add the hostname of the Knox Gateway and Hue Load Balancer hostname in the trusted origin and as a Knox Proxy host. For more information, see Integrate with Knox.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.7.1 CHF4 (version: 7.7.1-38008529)

- **OPSAPS-66197**

  Snapshot diff-based (incremental) HDFS to HDFS replication might corrupt destination directory structure when:

  - there is a source side HDFS move/rename operation.
  - the (move/rename) target on the replication destination is an existing unexpected directory.

  OPSAPS-63724 introduced an optional workaround where the target-side directory creations are ignored. When a colliding source-side move is expected both workarounds are recommended to be activated.

  Workaround:

  - Set the HDFS service core-site.xml advanced configuration snippet (also called safety valve) (on the destination side) "com.cloudera.enterprise.distcp.overwrite-merge-existing-rename-targets.enabled" to "true". (Note that enabling the workaround in OPSAPS-63724 uses a different advanced configuration snippet).
  - In an incremental replication run, check the stderr log of the last "Trigger a HDFS replication job on one of the available HDFS roles." step and make sure that the INFO distcp.DistCpSync: Overwrite merge of already existing move targets is enabled message is displayed.

  Usage notes:

  - When there is a conflicting replicated source side move/rename operation where - on the destination side - the target exists, there will be a merge attempt:
  - When the source side moved path is a directory and the conflicting destination side path is also a directory their contents will be merged.
  - When the destination side conflicting path is a file it will be overwritten by the replicated move.
  - When the source side moved path is a file the destination side conflicting path will be overwritten by the replicated move.
  - In case of other failures replication is expected to fall back to bootstrap (full file listing) run.

  Details of merge activity (when there is a conflicting path) is logged in the same stderr log with messages containing INFO distcp.DistCpSync$OverwriteMergeRenameBehavior.
- **OPSAPS-66160: Upgraded XStream version**

  The XStream version is upgraded to 1.4.20 version to fix CVE-2022-41966 issue.
- **OPSAPS-65958**

  After a Hive ACID replication policy is deleted, the database in the replication policy cannot be deleted from the source cluster. This issue is fixed.
- **OPSAPS-65870: Log4J 1.2.17 replaced with Reload4J**

  In this release, Cloudera has replaced all Apache Log4j 1.2.x logging libraries included with Cloudera Manager 7.7.1 Cumulative hotfix 3 with equivalent Reload4j libraries.
- **OPSAPS-65733**

  The following issues are fixed:

  - Import script incorrectly returns "0" for an unsuccessful import operation.
  - Dry run import of Ranger policies fails.
  - Import operation fails because of deadlock.
- **OPSAPS-64925**

  You could configure the numListstatusThreads parameter, that specifies the number of threads to be used for fetching the file statuses, only through CLI and not during the HDFS replication policy creation process. This issue is fixed.

  You can now configure this parameter during HDFS replication policy creation using the Advanced File listing threads field.

- **OPSAPS-63930**

  By default, snapshot diff-based (incremental) HDFS - HDFS replication uses a temp directory, created in the parent of replication destination directory to synchronize source-side rename and delete operations: deleted and renamed paths are first moved into this temporary directory, then the renamed ones will be moved to their target followed by the deletion of this temporary directory (thus deleting the paths scheduled to be deleted). Note that OPSAPS-63759 provides an optional behavior to execute individual deletes without these moves.

  This behavior of incremental replication leads to failure and fallback to bootstrap (full file listing) replication when the replication process can not create this temporary directory (due to restrictive HDFS permissions) or when the replication destination contains one or more HDFS encryption zones (because HDFS moves can not cross encryption zone boundary).

  This optional workaround solves these problems by executing rename operations in-place when possible, otherwise using the best possible temporary rename operations without the need of the above mentioned common temporary directory. Note that this workaround can be considered as a superset of OPSAPS-63759. That is when both are enabled, the current one is applied.

  Activating this workaround:

  - Set HDFS service core-site.xml advanced configuration snippet (on the destination side) "com.cloudera.enterprise.distcp.direct-rename-and-delete.enabled" to "true".
  - In an incremental replication run, check the stderr log of the last "Trigger a HDFS replication job on one of the available HDFS roles." step, and make sure the INFO distcp.DistCpSync: Will use direct rename and delete (for non cloud target) when using snapshot diff based sync. Temp directory creation on the target will be skipped. message is displayed.

  Adjusting delete logging: By default, every 100000 direct delete operations executed by this workaround are logged. This is useful for following the synchronization of large source side deletes. This default interval can be overridden by setting the "com.cloudera.enterprise.distcp.direct-delete.log-interval" advanced configuration snippet to an integer value greater than 0. Note that this advanced configuration snippet is shared with a workaround in OPSAPS-63759.

  Usage notes: There can be conflicting source side renames and rename - delete interactions when their destination side replay need to use temporary renames (for example, a name swap between two paths using three renames). For these cases, the temporary rename destination will typically be next to the final rename destination (will share the same parent path) avoiding both above mentioned failure scenarios. Such temporary renames will be logged during execution like:

  ```
  distcp.DistCpSync: Executing a temp rename: /test-repl-target/te
  st-repl-source/file2 -> /test-repl-target/test-repl-source/file2
  748016654
  ```

  After execution, the number of operations will also be logged like:

  ```
  INFO distcp.DistCpSync: Synced 0 through-tmp/cloud rename(s) and
   0 through-tmp delete(s) to target.
  INFO distcp.DistCpSync: Synced 2 direct delete(s) to target.
  INFO distcp.DistCpSync: Synced 2 direct rename(s) to target.
  INFO distcp.DistCpSync: Used 2 additional temporary rename(s)
  during syncing.
  ```

- **OPSAPS-63724**

  By default, the snapshot diff-based (incremental) HDFS - HDFS replication falls back to bootstrap (full file listing / FFL) replication when there are unexpected target-side changes. By enabling this workaround, certain target-side changes are tolerated by incremental replication without falling back to FFL. Note that when source side HDFS moves are expected to be synchronized the workaround mentioned in OPSAPS-66197 is recommended to be activated.

Activating this workaround:

- Set "com.cloudera.enterprise.distcp.check-for-safe-to-merge-target-side-changes.enabled" to "true" in the "YARN Service Advanced Configuration Snippet (Safety Valve) for core-site.xml" on the destination side, and then restart the stale services / redeploy client configuration. (Note that enabling OPSAPS-66197 uses a different advanced configuration snippet).
- In an incremental replication run, check the stderr log of the first "Run Pre-Filelisting Check" and make sure the INFO   distcp.PreCopyListingCheck: Check for safe to ignore (merge) targ et side   changes is enabled. message appears.

Usage notes:

- When a safe-to-ignore target change is found, "Run Pre-Filelisting Check" prints the following messages to its stderr log:

```
INFO util.DistCpUtils: There are changes on target, falling
back to regular distcp
NFO distcp.PreCopyListingCheck: The changes on target are safe
 to ignore.
INFO distcp.PreCopyListingCheck: Note that it is up to the
downstream processing steps if it falls back to full file li
sting or continue with snapshot diff execution
INFO distcp.PreCopyListingCheck: Changes to target: true
INFO distcp.PreCopyListingCheck: Changes to target are safe to
 ignore: true
```

- When target changes are not found safe-to-ignore, then the details about the reason appears in the messages:

```
INFO distcp.PreCopyListingCheck: Changes to target: true
INFO distcp.PreCopyListingCheck: Changes to target are safe
 to ignore: false
```

Allowed changes:

The following destination side changes (snapshot diff entries) are considered safe-to-ignore when this workaround is enabled:

- Additions (+): only if they are empty directories or contain only directories, all present on the source as directory.
- Deletions (-): only the source side path also missing.
- Modifications (M): must have an immediate, allowed (+) or (-) child path.

- **OPSAPS-63571**

  Sometimes, entries reported by the HDFS snapshot-diff report for deleted directories appear as modified. This might raise an FileNotFoundException error. In this scenario, you can configure the "com.cloudera.enterprise.distcp.hdfs-snapshot-diff-cleanup.enabled" advanced configuration snippet to address these unexpected entries.

- **OPSAPS-63529**

  The "deleteLatestSourceSnapshotOnJobFailure" HDFS policy property could be accessed only using CLI. You can now configure this parameter during HDFS replication policy creation using the Advanced Restart replication using non-incremental (bootstrap) replication on replication failure field.

- **OPSAPS-63362**

  Hive ACID replication policies failed if the source and target clusters have the same HDFS nameservice. This issue is fixed.

- **OPSAPS-63031**

  To provide a custom YARN queue for the Replication Metrics Getter command, the administrator can now specify the HIVE_REPL_METRICS_TEZQUEUE_NAME = _[***CUSTOM YARN QUEUE NAME***]_ key-value pair in the "Hive Replication Environment Advanced Configuration Snippet (Safety Valve)" for the Hive_on_tez service.

  On the next run, the replication metrics command uses the custom yarn queue for its execution.
- **OPSAPS-63030**

  The “Hive replication metrics getter” process failed for some Hive ACID replication policies because the TLS parameters were repeated in the JDBC URL. This issue is fixed.
- **OPSAPS-62612**

  The fix for this issue ensures that Replication Manager shows a warning message if there are any Hive ACID tables in the chosen database when you choose an external-tables-only database for a Hive external table replication policy.
- **OPSAPS-62886**

  When there are a large number of replication policies, the Cloudera Manager Replication Manager Replication Policies page takes a long time to load. This issue is fixed.
- **OPSAPS-63262**

  The “Hive on Tez Replication Metrics Getter” commands failed when there were long messages in the replication_metrics table. This issue is fixed.
- **OPSAPS-65419: Hosts page takes too long to load on large clusters**

  The All Hosts page sometimes takes more than 10 seconds and is very slow when Cloudera Manager manages a very large cluster such as about a hundred hosts. This performance problem is fixed now by reducing the number of SQLs made to the database. The page load time is now reduced dramatically.
- **OPSAPS-63077: Fix commissioning/recommissioning NodeManager failure in YARN**

  When the yarn.scheduler.configuration.store.class property is set to zk and YARN Queue Manager is not installed and enabled in a cluster every YARN node decommission causes an exception. With this fix, no refreshQueues command is called when ZooKeeper configuration store is used, but YARN Queue Manager is not.
- **OPSAPS-65242**

  Fixed an issue where an Event Server cleanup did not work properly and now it works as intended, uses less CPU and keeps the events within the requested limits.
- **OPSAPS-66022**

  When a Hive ACID replication policy run is skipped, the replication policy status incorrectly shows Failed or Error. This issue is fixed.
- The repositories for Cloudera Manager 7.7.1-CHF4 are listed in the following table:

Table 25: Cloudera Manager 7.7.1-CHF4

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-38008529/ubuntu1804/apt/cloudera-manager.list`

Cloudera Manager 7.7.1 Cumulative hotfix 3

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 3.

This cumulative hotfix was released on December 14, 2022.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF3 (version: 7.7.1-34818722):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
    - Name = hadoop.security.group.mapping.ldap.bind.password
    - Value = (Enter the LDAP bind password here)
    - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:
Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixes that were shipped for Cloudera Manager 7.7.1 CHF3 (version: 7.7.1-34818722):

- OPSAPS-65342 - Missing FIPS knox-Cloudera Manager configuration in 7.1.7 SP2
- OPSAPS-65652 - Fix additional IBM PPC build failures after GitHub upgrade.

- CDPD-46532 - For HA HDFS deployments, WebHDFS failover is not configured in the Knox topology, so requests directed to stand-by HDFS nodes are failing instead of failing-over to an active node.

  The repositories for Cloudera Manager 7.7.1-CHF3 are listed in the following table:

Table 26: Cloudera Manager 7.7.1-CHF3

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/sles12/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/ubuntu2004/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/ubuntu1804/apt`
	Repository file:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/ubuntu1804/apt/cloudera-manager.list`

IBM PowerPC RHEL 8	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat8-ppc/yum`
IBM PowerPC RHEL 7	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm7/patch/7.7.1-34818722/redhat7-ppc/yum`

Cloudera Manager 7.7.1 Cumulative hotfix 2

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 2.

This cumulative hotfix was released on November 28, 2022.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF2 (version: 7.7.1-34281315):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/j
ava-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openj
dk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixes that were shipped for Cloudera Manager 7.7.1 CHF2 (version: 7.7.1-34281315):

- OPSAPS-62511 - Upgrade jsoup due to CVE-2021-37714
- OPSAPS-62521 - Upgrade snakeyaml to 1.31 due to CVE-2017-18640, CVE-2022-25857, CVE-2022-38749, CVE-2022-38751, and CVE-2022-38750
- OPSAPS-63984 - Upgrade commons-io to 2.11.0 due to CVE-2021-29425
- OPSAPS-64032 - Upgrade poi to 5.2.2 due to CVE-2022-26336
- OPSAPS-64080 - Upgrade requests to 2.27.1 due to CVE-2018-18074
- OPSAPS-64082 - Upgrade esapi-java-legacy to 2.4.0.0 due to CVE-2022-23457, and CVE-2022-24891
- OPSAPS-64654 - Multiple Critical CVEs for jackson-databind in the most recent scan report for CM 7.6.2 and CM 7.8.0
- OPSAPS-65098 - Update logredactor to 2.0.14 due to CVEs in jackson-databind
- OPSAPS-62805 - Extend Log search feature for the log4j2
- OPSAPS-64153 - Core Settings service is getting added twice during cluster provisioning using clustertemplateimportcommand in data hub.
- OPSAPS-64614 - Cloudera Manager server fails to complete the upgrade and will not start, if a cluster had a legacy Core Configuration service with any number of Storage Operations roles.
- OPSAPS-64655 - Performance issues in loading and using Hue
- OPSAPS-64744 - NPE in Cloudera Manager upgrade if StubDFS created but no StorageOps roles present
- OPSAPS-65040 - ImpalaFileFormatAnalysisRule should only inspect SCAN_NODE
- OPSAPS-65064 - Prevents importing a cluster template containing a base cluster with a service of type CORE_SETTINGS.

- OPSAPS-65143 - NPE in RulesCluster.java:169 when adding Cloudera Management services

  The repositories for Cloudera Manager 7.7.1-CHF2 are listed in the following table:

Table 27: Cloudera Manager 7.7.1-CHF2

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/redhat8/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/redhat7/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/sles12/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/ubuntu2004/apt`
	Repository file:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/ubuntu1804/apt`
	Repository file:
	`http://USERNAME:PASSWORD@bits.cloudera.com/5b3fb4b4/patch-5579/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.7.1 CHF2 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

Cloudera Manager 7.7.1 Cumulative hotfix 1

Know more about the Cloudera Manager 7.7.1 cumulative hotfixes 1.

This cumulative hotfix was released on October 28, 2022.

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

Following are the list of known issues and their corresponding workarounds that are shipped for Cloudera Manager 7.7.1 CHF1 (version: 7.7.1-33209161):

OPSAPS-68689: Unable to emit the LDAP Bind password in core-site.xml for client configurations

If the CDP cluster has LDAP group to OS group mapping enabled, then applications running in Spark or Yarn would fail to authenticate to the LDAP server when trying to use the LDAP bind account during the LDAP group search.

This is because the LDAP bind password was not passed to the /etc/hadoop/conf/core-site.xml file. This was intended behavior to prevent leaking the LDAP bind password in a clear text field.

Set the LDAP Bind password through the HDFS client configuration safety valve.

1. On the Cloudera Manager UI, navigate to the HDFS service, by clicking on the HDFS service under the Cluster.
2. Click the Configuration tab. Search for the HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml configuration parameter.
3. Add an entry with the following values:
   - Name = hadoop.security.group.mapping.ldap.bind.password
   - Value = (Enter the LDAP bind password here)
   - Description = Password for LDAP bind account
4. Then click the Save Changes button to save the safety valve entry.
5. Perform the instructions from the Manually Redeploying Client Configuration Files to manually deploy client configuration files to the cluster.

OPSAPS-68452: Azul Open JDK 8 and 11 are not supported with Cloudera Manager

Azul Open JDK 8 and 11 are not supported with Cloudera Manager. To use Azul Open JDK 8 or 11 for Cloudera Manager RPM/DEBs, you must manually create a symlink between the Zulu JDK installation path and the default JDK path.

After installing Azul Open JDK8 or 11, you must run the following commands on all the hosts in the cluster:

Azul Open JDK 8

RHEL or SLES

```
# sudo ln -s /usr/lib/jvm/java-8-zulu-openjdk-jdk /usr/lib/jvm/java-8-openjdk
```

Ubuntu or Debian

```
# sudo ln -s /usr/lib/jvm/zulu-8-amd64 /usr/lib/jvm/java-8-openjdk
```

Azul Open JDK 11

For DEBs only

```
# sudo ln -s /usr/lib/jvm/zulu-11-amd64 /usr/lib/jvm/java-11
```

Following are the list of fixes that were shipped for Cloudera Manager 7.7.1 CHF1 (version: 7.7.1-33209161):

- OPSAPS-62886 - Do not fetch replication history for high replication policy count
- OPSAPS-63881 - Permissions of user directories under /var/lib/ is 700 on RHEL 8.4
- OPSAPS-63988 - Upgrade pdfbox to 2.0.24+ due to CVE-2021-31812, CVE-2021-27807, CVE-2021-27906, and CVE-2021-31811
- OPSAPS-64087 - Upgrade XercesImpl to 2.12.2 due to CVE-2022-23437, and CVE-2017-10355
- OPSAPS-64287 - DAS: Add extra application connector configs
- OPSAPS-64599 - The periodic HBase monitoring tasks and Service Monitor logs are flooded with NoClassDefFoundError error messages during the CDH 5 cluster management
- OPSAPS-64695 - Make SMON/HMON updates cleanup period configurable
- OPSAPS-64859 - The Replication History page does not load the history of the policy
- OPSAPS-64602 - Unsupported ciphersuite on FIPS upgrade in 7.1.8 CHF1

The repositories for Cloudera Manager 7.7.1-CHF1 are listed in the following table:

Table 28: Cloudera Manager 7.7.1-CHF1

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/redhat8/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/redhat7/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/sles12/yum`
	Repository File:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/ubuntu2004/apt`
	Repository file:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/ubuntu1804/apt`
	Repository file:
	`http://USERNAME:PASSWORD@bits.cloudera.com/f9ee612a/patch-5567/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.7.1 CHF1 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.