

Cloudera Manager 7.6.7

## Release Notes

Date published: 2020-11-30

Date modified: 2024-02-06

# CLOUDERA

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

# Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

<b>Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3).....</b>	<b>5</b>
What's New in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3).....	5
Fixed Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3).....	5
Known Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3).....	6
Documentation Errata in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3).....	7
Deprecation notices in Cloudera Manager 7.11.3 CHF4.....	7
Platform and OS.....	8
 <b>Cloudera Manager 7.6.7 Release Notes (CDP Private Cloud Base 7.1.7 SP2).....</b>	<b>8</b>
What's New in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2).....	8
Fixed Issues in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2).....	8
Known Issues in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2).....	10
Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2).....	13
Cumulative hotfixes.....	14
Cloudera Manager 7.6.7 Cumulative hotfix 13.....	14
Cloudera Manager 7.6.7 Cumulative hotfix 12.....	15
Cloudera Manager 7.6.7 Cumulative hotfix 11.....	17
Cloudera Manager 7.6.7 Cumulative hotfix 10.....	19
Cloudera Manager 7.6.7 Cumulative hotfix 9.....	20
Cloudera Manager 7.6.7 Cumulative hotfix 8.....	22
Cloudera Manager 7.6.7 Cumulative hotfix 7.....	24
Cloudera Manager 7.6.7 Cumulative hotfix 6.....	26
Cloudera Manager 7.6.7 Cumulative hotfix 5.....	28
Cloudera Manager 7.6.7 Cumulative hotfix 4.....	30
Cloudera Manager 7.6.7 Cumulative hotfix 3.....	33
Cloudera Manager 7.6.7 Cumulative hotfix 2.....	35
Cloudera Manager 7.6.7 Cumulative hotfix 1.....	37
 <b>Cloudera Manager 7.6.1 Release Notes (CDP Private Cloud Base 7.1.7 SP1).....</b>	<b>39</b>
What's New in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1).....	39
Fixed Issues in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1).....	39
Known Issues in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1).....	43
Documentation Errata in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1).....	46
Cumulative hotfixes.....	48
Cloudera Manager 7.6.1 Cumulative hotfix 9.....	48
Cloudera Manager 7.6.1 Cumulative hotfix 8.....	50
Cloudera Manager 7.6.1 Cumulative hotfix 7.....	52
Cloudera Manager 7.6.1 Cumulative hotfix 6.....	54
Cloudera Manager 7.6.1 Cumulative hotfix 5.....	56
Cloudera Manager 7.6.1 Cumulative hotfix 4.....	58
Cloudera Manager 7.6.1 Cumulative hotfix 3.....	60

Cloudera Manager 7.6.1 Cumulative hotfix 2..... 61

Cloudera Manager 7.6.1 Cumulative hotfix 1..... 63

**Cloudera Manager 7.4.4 Release Notes.....65**

What's New in Cloudera Manager 7.4.4.....65

Fixed Issues in Cloudera Manager 7.4.4..... 68

Known Issues in Cloudera Manager 7.4.4.....69

Known Issues for IBM PowerPC.....72

## Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3)

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

### What's New in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3)

New features and changed behavior for Cloudera Manager 7.11.3 Cumulative hotfix 4.

There are no new features in Cloudera Manager 7.11.3 Cumulative hotfix 4 release. For any significant updates, see the [Documentation Errata in Cloudera Manager 7.11.3 Cumulative hotfix 4 \(CDP Private Cloud Base 7.1.7 SP3\)](#) on page 7.

### Fixed Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3)

Fixed issues in Cloudera Manager 7.11.3 Cumulative hotfix 4.

**OPSAPS-69387: Update Spark 3 parcel CSD's repository URL to point to CDP 7.1.9.x cluster in CM**

Updated the Spark 3 parcel's repository URL to point to <https://archive.cloudera.com/p/spark3/3.3.7190.0/parcels/> instead of <https://archive.cloudera.com/p/spark3/3.3.7180.0/parcels/>.

**OPSAPS-69458: Custom properties atlas.jaas.KafkaClient.option.password appears in a clear text in CDP cluster services.**

CDP Private Cloud Base 7.1.9 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-69480: Hardcode MR add-opens-as-default config**

Cloudera Manager uses fixed runtime versions when determining clients, instead of using the one connected to the deployed runtime version, which can cause issues. During an upgrade if an app is submitted with a client containing MAPREDUCE-7449 to a runtime that doesn't contain MAPREDUCE-7449's related changes, the application submission fails. To fix this issue MAPREDUCE-7468 changes the default behaviour of the feature to avoid including the placeholder by default. Cloudera Manager has a hardcoded property from the runtime versions where the replacement is correctly done in NM code.

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

Cloudera Manager now registers kafka\_connect\_connector\_task\_metrics\_batch\_size\_avg and kafka\_connect\_connector\_task\_metrics\_batch\_size\_max metrics correctly.

**OPSAPS-69556: While upgrading from CDP Private Cloud Data Services 1.5.1 to 1.5.2, the public registry with public bits fails with ImagePull Errors, and the docker registry modified to point to docker-private during the upgrade**

Previously, when upgrading using the Cloudera public registry with public bits, the Docker registry would incorrectly change to point to docker-private.infra.cloudera.com. This issue is now fixed to point to the correct registry.

**OPSAPS-69357: Yarn application bundle script needs to be backwards compatible with python 2.7.**

Application bundle collection has been fixed to support both Python2 and Python3 environments.

**OPSAPS-68288: Cloudera Manager waits on "Refreshing Resource manager" during the time when the node-manager is being decommissioned**

The decommission now works as expected.

**OPSAPS-69502: Upgrade failures from CDH6 to 7.1.7 SP3 because ACL is not the expected for znnode**

Updated the zk-client.sh to follow the output change of the ZK CLI during upgrade so that the upgrade no longer fails.

## Known Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3)

Known issues in Cloudera Manager 7.11.3 Cumulative hotfix 4.

**OPSAPS-68340: Zeppelin paragraph execution fails with the User not allowed to impersonate error.**

Starting from Cloudera Manager 7.11.3, Cloudera Manager auto-configures the livy\_admin\_users configuration when Livy is run for the first time. If you add Zeppelin or Knox services later to the existing cluster and do not manually update the service user, the User not allowed to impersonate error is displayed.

If you add Zeppelin or Knox services later to the existing cluster, you must manually add the respective service user to the livy\_admin\_users configuration in the Livy configuration page.

**OPSAPS-69342: Access issues identified in MariaDB 10.6 were causing discrepancies in High Availability (HA) mode**

MariaDB 10.6, by default, includes the property require\_secure\_transport=ON in the configuration file (/etc/my.cnf), which is absent in MariaDB 10.4. This setting prohibits non-TLS connections, leading to access issues. This problem is observed in High Availability (HA) mode, where certain operations may not be using the same connection.

To resolve the issue temporarily, you can either comment out or disable the line require\_secure\_transport in the configuration file located at /etc/my.cnf.

**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-62834: Status of the deleted table is seen as ACTIVE in Atlas after the completion of navigator2atlas migration process**

The status of the deleted table displays as ACTIVE.

None

**CDPD-62837: During the navigator2atlas process, the hive\_storagedesc is incomplete in Atlas**

For the hive\_storagedesc entity, some of the attributes are not getting populated.

None

**OPSAPS-69897: NPE in Ozone replication from CM 7.7.1 to CM 7.11.3**

When you use source Cloudera Manager 7.7.1 and target Cloudera Manager 7.11.3 for Ozone replication policies, the policies fail with Failure during PreOzoneCopyListingCheck execution: null error. This is because the target Cloudera Manager 7.11.3 does not retrieve the required source bucket information for validation from the source Cloudera Manager 7.7.1 during the PreCopyListingCheck command phase. You come across this error when you use source Cloudera Manager versions lower than 7.10.1 and target Cloudera Manager versions higher than or equal to 7.10.1 in an Ozone replication policy.

Upgrade the source Cloudera Manager to 7.11.3 or higher version.

## Documentation Errata in Cloudera Manager 7.11.3 Cumulative hotfix 4 (CDP Private Cloud Base 7.1.7 SP3)

You must be aware of the platform support for the Cloudera Manager 7.11.3 CHF4 release.

**Platform Support Enhancements**

- New OS support:
  - RHEL 8.10
  - Oracle 8.10 (supported with Red Hat Compatible Kernel (RHCK) only)
- New DB Versions: MariaDB 10.11 (LTS)
- New JDK Version: There are no changes for JDK support in this release.

**FIPS support for JDK11 in Zeppelin**

Added FIPS support for JDK11 in Zeppelin.

## Deprecation notices in Cloudera Manager 7.11.3 CHF4

Certain features and functionalities have been removed or deprecated in Cloudera Manager 7.11.3 CHF4. You must review these items to understand whether you must modify your existing configuration. You can also learn about the features that will be removed or deprecated in the future release to plan for the required changes.

**Terminology**

Items in this section are designated as follows:

**Deprecated**

Technology that Cloudera is removing in a future Cloudera Manager release. Marking an item as deprecated gives you time to plan for removal in a future Cloudera Manager release.

**Moving**

Technology that Cloudera is moving from a future Cloudera Manager release and is making available through an alternative Cloudera offering or subscription. Marking an item as moving gives you time to plan for removal in a future Cloudera Manager release and plan for the alternative Cloudera offering or subscription for the technology.

**Removed**

Technology that Cloudera has removed from Cloudera Manager and is no longer available or supported as of this release. Take note of technology marked as removed since it can potentially affect your upgrade plans.

## Platform and OS

The listed Operating Systems and databases are deprecated or removed from the Cloudera Manager 7.11.3 CHF4 release.

### Database Support:

The listed databases are deprecated from the Cloudera Manager 7.11.3 CHF4 release.

- Postgres 11

### Operating System

None

## Cloudera Manager 7.6.7 Release Notes (CDP Private Cloud Base 7.1.7 SP2)

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



**Important:** Do not upgrade to Cloudera Manager 7.6.7 if you are running CDP Private Cloud Data Services in your deployment.

## What's New in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2)

New features and changed behavior for Cloudera Manager 7.6.7.

There are no new features 7.1.7 SP2 (Cloudera Manager 7.6.7) release.

## Fixed Issues in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2)

Fixed issues in Cloudera Manager 7.6.7



**Important:** Do not upgrade to Cloudera Manager 7.6.7 if you are running CDP Private Cloud Data Services in your deployment.

### 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-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.



**OPSAPS-65040: ImpalaFileFormatAnalysisRule should only inspect SCAN\_NODE**

Fixed slow impala query processing by Cloudera Manager SMON. This fix improves the performance of ImpalaFileFormatAnalysisRule.

**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-64599: The Service Monitor logs are flooded with error messages during the CDH 5 cluster management**

Fixed an issue where a dependency conflict prevents periodic HBase monitoring tasks, and Service Monitor logs are flooded with NoClassDefFoundError errors when Cloudera Manager is managing a CDH 5 cluster.

**OPSAPS-64187: Cloudera Manager Event Server does not clean up old events**

Fixed an issue where an Event Server cleanup did not work and was unable to clean the old events.

**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.

**OPSAPS-63605: An Event Server cannot start after an upgrade due to a field type mismatch**

Fixed an issue where, in case of sufficiently long event attributes, a deprecated field type is replaced with an incompatible field type in the backing data store as part of the Cloudera Manager upgrade. This prevents the Event Server from starting. This fix changes the field type to a compatible one.

**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-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-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.

**OPSAPS-63759: Optional direct delete in DistCp snapshot-diff based replication**

When the accumulated temporary file count in a HDFS temporary folder (snapshot diff-based HDFS replication synchronizes the deletes and renames through a temporary directory on the target

cluster) crosses the HDFS directory entry count limit per directory of ~6.4 items, the incremental replication fails and the replication process falls back to bootstrap replication (that is, all the files are replicated).

OPSAPS-63759 introduces an optional direct delete behavior where delete operations are run directly without the intermediate moves into the common temporary directory. To enable this workaround:

1. Go to the target Cloudera Manager Clusters *HDFS service* Configuration tab.
2. Search for the Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml property.
3. Add the `com.cloudera.enterprise.distcp.direct-rename-and-delete.enabled=true` key-value pair.

This parameter activates the direct delete approach.

Optionally, you can set the `com.cloudera.enterprise.distcp.direct-delete.log-interval=[***enter a value (n) greater than 0***]` key-value pair to override the default (100000) delete count for each delete progress log message.



**Note:** If you update these parameters after the HDFS file limit per directory is crossed, the next replication policy run is a bootstrap operation (that is, all the files are replicated and snapshot-diffs are not used). Snapshot diffs (or incremental replication) are used only after a successful bootstrap run. Note that the activation of this workaround can be followed in the logs printed by DistCp.

#### **OPSAPS-62886: Replication Policies page takes a longer time to load when the replication policy count is high**

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.

## **Known Issues in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2)**

Known issues in Cloudera Manager 7.6.7

#### **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-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-66021: Error message about an unsupported ciphersuite while upgrading cluster with the latest FIPS compliance**

When attempting to display the YARN Queue Manager interface, Cloudera Manager displays the following error message:

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

Ciphersuites supported by Query Manager and JVM are not matching with the ciphersuites that are selected in Nmap, especially with ciphersuites that contain 3DES.

To avoid selecting ciphersuites that contains 3DES and to address the exception:

1. SSH into the Cloudera Manager server as a root user.
2. In the `/etc/default/cloudera-scm-server` file, remove the ciphers which contains 3DES from the `CMF_OVERRIDE_TLS_CIPHERS` line.
3. You can uncomment and remove the ciphers which contains 3DES from the below key-value pair list:

```
#export CMF_OVERRIDE_TLS_CIPHERS="TLS_ECDHE_ECDSA_WITH_AES_1
28_GCM_SHA256:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256:TLS_ECDH
E_ECDSA_WITH_AES_256_GCM_SHA384:TLS_ECDHE_RSA_WITH_AES_256_G
CM_SHA384:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256:TLS_DHE_RSA_WI
TH_AES_256_GCM_SHA384:TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA25
6:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256:TLS_ECDHE_ECDSA_WITH
_AES_128_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384:TLS_E
CDHE_RSA_WITH_AES_128_CBC_SHA:TLS_ECDHE_ECDSA_WITH_AES_256_C
```

```
BC_SHA384:TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_128_CBC_SHA256:TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA256:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA:TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA:TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA:TLS_RSA_WITH_AES_128_GCM_SHA256:TLS_RSA_WITH_AES_256_GCM_SHA384:TLS_RSA_WITH_AES_128_CBC_SHA256:TLS_RSA_WITH_AES_256_CBC_SHA256:TLS_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_256_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA"
```

4. The updated key-value pair list might display as below:

```
export CMF_OVERRIDE_TLS_CIPHERS="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256:TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256:TLS_DHE_RSA_WITH_AES_256_GCM_SHA384:TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256:TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384:TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384:TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA:TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_128_CBC_SHA256:TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA256:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:TLS_RSA_WITH_AES_128_GCM_SHA256:TLS_RSA_WITH_AES_256_GCM_SHA384:TLS_RSA_WITH_AES_128_CBC_SHA256:TLS_RSA_WITH_AES_256_CBC_SHA256:TLS_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_256_CBC_SHA"
```

5. Restart Cloudera Manager.

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

#### **OPSAPS-66090: Error message while running collect stack traces (jstack) command in an upgraded cluster**

When running the collect stack traces (jstack) command in an upgraded cluster, Cloudera Manager displays the following error message:

Failed to execute jstack.

Run the Java jstack utility to capture Java thread stack traces.

Process HDFS-DATANODE-jstack (id=251) on host quasar-dasifj-1.quasar-dasifj.root.hwx.site (id=2) exited with 1 and expected 0

After you upgrade the cluster, restart the cluster. This action should switch the re-parented processes to direct control and re-synchronization process IDs to Cloudera Manager server.

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

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

Cloudera Manager does not allow you to set to "0" for the dfs\_access\_time\_precision and dfs\_name\_node\_accesstime\_precision configuration parameters.

You will not be able to update dfs\_access\_time\_precision and dfs\_namenode\_accesstime\_precision to "0". If you try to enter "0" in these configuration input fields, then the field gets cleared off and results in a validation error: This field is required.

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

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

#### **OPSAPS-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.

## Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.6.7 (CDP Private Cloud Base 7.1.7 SP2)

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

- CVE-2023-20860
- CVE-2023-20861
- CVE-2022-40152
- CVE-2021-22112
- CVE-2022-31197
- CVE-2022-21724
- CVE-2022-40149
- CVE-2022-40150
- CVE-2018-18074
- CVE-2017-18640
- CVE-2022-25857
- CVE-2022-38749
- CVE-2022-38751
- CVE-2022-38750
- CVE-2022-36033
- CVE-2020-11988
- CVE-2022-23437
- CVE-2022-23457
- CVE-2022-24891
- CVE-2021-31812
- CVE-2021-27807
- CVE-2021-27906
- CVE-2021-31811
- CVE-2021-37714
- CVE-2020-28491
- CVE-2021-39141
- CVE-2021-39152
- CVE-2021-39148
- CVE-2021-29505
- CVE-2021-39146
- CVE-2021-39139
- CVE-2021-39147
- CVE-2021-39149
- CVE-2021-39150
- CVE-2021-39145
- CVE-2021-39144
- CVE-2021-39154
- CVE-2021-39151

- CVE-2021-39153
- CVE-2022-23307
- CVE-2022-23305
- CVE-2022-23302
- CVE-2021-4104
- CVE-2020-11979
- CVE-2021-36374
- CVE-2021-36373
- CVE-2020-9488

## Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.6.7.

### Cloudera Manager 7.6.7 Cumulative hotfix 13

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 13.

This cumulative hotfix was released on February 1, 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 7.6.7 CHF13 (version: 7.6.7-h15-49714782):**

**OPSAPS-69635: On selecting a source peer whose CM API version supports "File listing threads (numFetchThreads)" the UI option to update 'File listing threads' is not visible**

During the HDFS replication policy creation process, the Resources File listing threads option does not appear even though the source cluster's Cloudera Manager API version supports the option.

This issue appears when the source and target Cloudera Manager versions are different. Ensure that you upgrade both the clusters' Cloudera Manager to a CHF release that supports reporting to other peers that the source peer supports the File listing threads option. For example, you can upgrade both the clusters' Cloudera Manager to 7.6.7 CHF12, 7.7.1 CHF17, or 7.11.3 CHF2 or higher versions.

The repositories for Cloudera Manager 7.6.7-CHF13 are listed in the following table:

**Table 1: Cloudera Manager 7.6.7-CHF13**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/redhat8/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/7.6.7-h15-49714782/ubuntu1804/apt/cloudera-manager.list</pre>

### 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 7.6.7 Cumulative hotfix 12

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 12.

This cumulative hotfix was released on December 15, 2023.



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

**New features and changed behavior for Cloudera Manager 7.6.7 CHF12 (version: 7.6.7-h14-48043553):**

**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)

**Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.3 CHF2 (version: 7.6.7-h14-48043553):****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-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.

The repositories for Cloudera Manager 7.6.7-CHF12 are listed in the following table:

**Table 2: Cloudera Manager 7.6.7-CHF12**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/sles12/yum/cloudera-manager.repo</pre>



Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h14-48043553/ubuntu1804/apt/cloudera-manager.list</pre>

### 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 7.6.7 Cumulative hotfix 11

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 11 (version: 7.6.7-h13-46891257).

This cumulative hotfix was released on November 9, 2023.



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

The repositories for Cloudera Manager 7.6.7-CHF11 are listed in the following table:

**Table 3: Cloudera Manager 7.6.7-CHF11**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/ubuntu1804/apt/cloudera-manager.list</pre>
IBM PowerPC RHEL 7	<pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat7-ppc/yum</pre>
IBM PowerPC RHEL 8	<pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h13-46891257/redhat8-ppc/yum</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 10

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 10.

This cumulative hotfix was released on October 9, 2023.



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

Following are the list of fixed issues that were shipped for Cloudera Manager 7.6.7 CHF10 (version: 7.6.7-h12-45722147)

### **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.

The repositories for Cloudera Manager 7.6.7-CHF10 are listed in the following table:

**Table 4: Cloudera Manager 7.6.7-CHF10**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/redhat8/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h12-45722147/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 9

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 9.

This cumulative hotfix was released on September 21, 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 7.6.7 CHF8 (version: 7.6.7-h10-45231598):**

**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
```

The repositories for Cloudera Manager 7.6.7-CHF9 are listed in the following table:

**Table 5: Cloudera Manager 7.6.7-CHF9**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/sles12/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h10-45231598/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 8

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 8.

This cumulative hotfix was released on July 19, 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 7.6.7 CHF8 (version: 7.6.7-h8-43190985):

### 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 7.6.7 CHF8 (version: 7.6.7-h8-43190985):**

**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-67478: Upgraded Spring Framework version**

The Spring Framework version is upgraded to 5.3.27 version to fix CVE issues.

**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.

The repositories for Cloudera Manager 7.6.7-CHF8 are listed in the following table:

**Table 6: Cloudera Manager 7.6.7-CHF8**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/ubuntu1804/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h8-43190985/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 7

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 7.

This cumulative hotfix was released on June 27, 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 7.6.7 CHF7 (version: 7.6.7-h7-42198279):

### 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 7.6.7 CHF7 (version: 7.6.7-h7-42198279):

### 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.

The repositories for Cloudera Manager 7.6.7-CHF7 are listed in the following table:



**Table 7: Cloudera Manager 7.6.7-CHF7**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/ubuntu1804/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/ubuntu1804/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
IBM PowerPC RHEL 8	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat8-ppc/yum</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat8-ppc/yum/cloudera-manager.repo</pre>
IBM PowerPC RHEL 7	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat7-ppc/yum</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h7-42198279/redhat7-ppc/yum/cloudera-manager.repo</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 6

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 6.

This cumulative hotfix was released on June 8, 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 7.6.7 CHF6 (version: 7.6.7-h6-41705718):

### 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 7.6.7 CHF6 (version: 7.6.7-h6-41705718):

**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.

The repositories for Cloudera Manager 7.6.7-CHF6 are listed in the following table:

**Table 8: Cloudera Manager 7.6.7-CHF6**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/ubuntu1804/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h6-41705718/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 5

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 5.

This cumulative hotfix was released on April 24, 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 7.6.7 CHF5 (version: 7.6.7-h5-40213482)::

### 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 7.6.7 CHF5 (version: 7.6.7-h5-40213482):

- 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 7.6.7-CHF5 are listed in the following table:

**Table 9: Cloudera Manager 7.6.7-CHF5**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/ubuntu1804/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h5-40213482/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 4

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 4.

This cumulative hotfix was released on March 30, 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 7.6.7 CHF4 (version: 7.6.7-h4-39231315):

### 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 7.6.7 CHF4 (version: 7.6.7-h4-39231315):

- 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-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-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/test-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-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-65966**

Fixed an issue where Ranger policies were not automatically created for Kudu.

- **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 7.6.7-CHF4 are listed in the following table:

**Table 10: Cloudera Manager 7.6.7-CHF4**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/sles12/yum/cloudera-manager.repo</pre>



Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h4-39231315/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 3

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 3.

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 7.6.7 CHF3 (version: 7.6.7-h3-38745041):

### 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 7.6.7 CHF3 (version: 7.6.7-h3-38745041):

- **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-66050**

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.

The repositories for Cloudera Manager 7.6.7-CHF3 are listed in the following table:

**Table 11: Cloudera Manager 7.6.7-CHF3**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/sles12/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h3-38745041/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 2

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 2.

This cumulative hotfix was released on February 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 7.6.7 CHF2 (version: 7.6.7-h2-38250798):

### 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 7.6.7 CHF2 (version: 7.6.7-h2-38250798):

- **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 7.6.7-CHF2 are listed in the following table:

**Table 12: Cloudera Manager 7.6.7-CHF2**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/redhat8/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/redhat7/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/redhat7/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/sles12/yum</pre> Repository File: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/sles12/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h2-38250798/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.7 Cumulative hotfix 1

Know more about the Cloudera Manager 7.6.7 cumulative hotfixes 1.

This cumulative hotfix was released on February 16, 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 7.6.7 CHF1 (version: 7.6.7-h1-37647895):

### 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 7.6.7 CHF1 (version: 7.6.7-h1-37647895):

- **OPSAPS-64520**

Some CSD based service icons were missing. This issue is fixed now.

- **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-65562**

Enabling HBase snapshot export to Azure storage during HBase replication from CDH5 source cluster.

- **OPSAPS-65913**

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

The repositories for Cloudera Manager 7.6.7-CHF1 are listed in the following table:

**Table 13: Cloudera Manager 7.6.7-CHF1**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat8/yum">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat8/yum</a> Repository File: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat8/yum/cloudera-manager.repo">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat8/yum/cloudera-manager.repo</a>
RHEL 7 Compatible	Repository: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat7/yum">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat7/yum</a> Repository File: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat7/yum/cloudera-manager.repo">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/redhat7/yum/cloudera-manager.repo</a>
SLES 12	Repository: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/sles12/yum">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/sles12/yum</a> Repository File: <a href="https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/sles12/yum/cloudera-manager.repo">https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/sles12/yum/cloudera-manager.repo</a>

Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.7-h1-37647895/ubuntu1804/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.1 Release Notes (CDP Private Cloud Base 7.1.7 SP1)

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



**Important:** Do not upgrade to Cloudera Manager 7.6.1 if you are running CDP Private Cloud Data Services in your deployment.

### What's New in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1)

New features and changed behavior for Cloudera Manager 7.6.1.

There are no new features 7.1.7 SP1 (Cloudera Manager 7.6.1) release. For any significant updates, see the [Documentation Errata in Cloudera Manager 7.6.1 \(CDP Private Cloud Base 7.1.7 SP1\)](#) on page 46.

### Fixed Issues in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1)

Fixed issues in Cloudera Manager 7.6.1



**Important:** Do not upgrade to Cloudera Manager 7.6.1 if you are running CDP Private Cloud Data Services in your deployment.

#### Cloudera Bug: OPSAPS-23472: Fix inaccuracies in Report Manager quota cache

Due to the inaccuracy of the HDFS quotas, the quota cache has been disabled. The modified quota will appear in the usage reports after the new HDFS fsimage is processed.

#### Cloudera Bug: OPSAPS-57366: Cloudera Manager Sessions with Oracle database are not getting freed up

When using Cloudera Manager 7.x with Oracle Databases, Cloudera Manager may cause a storage leak in the Oracle database Temporary Space pool. This will cause the Temporary Space to fill up, causing some queries from all applications using that Temporary Space to fail. This fix ensures that the Temporary Space used by Cloudera Manager is released after each query.

**Cloudera Bug: OPSAPS-59359: Support secure web UIs without HDFS**

It was not possible to enable the Secure WEB UI for Yarn if the cluster did not have the HDFS service. Now the Secure WEB UI can be enabled with any DFS service in the cluster, including Dell EMC PowerScale. Similarly, now the HTTP authentication cookie domain can be configured for any DFS service."

**Cloudera Bug: OPSAPS-60943: Clicking on Historical Disk Usage by (User/Group) causes NPE**

Fixed an issue on the Reports page in the Cloudera Manager Admin Console. When clicking the link for Historical Disk Usage by (User or Group) the following error, caused by a Null Pointer Exception, appears: Server Error A server error has occurred. See the Cloudera Manager Server log for details.

**Cloudera Bug: OPSAPS-60949: Auto-TLS initialization should use FQDN instead of hostname**

Hosts now use the fully-qualified domain name (FQDN) instead of the hostname for certificate generation when enabling Auto TLS.

**Cloudera Bug: OPSAPS-61209: Alert publisher keeps logging "Connection Refused" for smtp server**

Disabled email alerts by default in Alert Publisher, preventing exceptions from being logged when default mail server settings are unsuitable for the deployment. Email alerts, if desired, have to be enabled manually. Notably, this also includes upgrades from Cloudera Manager versions that enable them by default.

**Cloudera Bug: OPSAPS-61235: Agent should run SS command only over IPv4**

The Cloudera Manager Agent uses the 'ss' command to detect port conflicts. This command fails with a segmentation fault when IPv6 is disabled on the host and causes error messages to flood in the logs. This fix resolves the issue by limiting 'ss' to obtain only IPv4 information for port detection.

**Cloudera Bug: OPSAPS-61286: Re-enable service log rotation after Cloudera Manager upgrade**

Fixed a bug that occurs when upgrading Cloudera Manager agents that caused service logging to fail.

**Cloudera Bug: OPSAPS-61326: Cluster installation on 7.1.7 with IBM PowerPC is failing while starting the Hive service**

Fixed an issue that caused the Hive Metastore to fail unless the "hive.metastore.transactional.event.listeners" configuration in the Hive Metastore Server Safety Valve was set. That configuration is no longer required.

**Cloudera Bug: OPSAPS-61408: KMS ACL rendering needs improvements**

When the set of KMS ACLs is very large, editing it on the configuration page is not feasible. The ACLs editing page now displays a text area instead.

**Cloudera Bug: OPSAPS-61482: Generate Credentials (MIT) script is hiding errors**

Resolved issue where generating MIT Kerberos credentials may fail, but no script output is observed.

**Cloudera Bug: OPSAPS-61549: Filter Hive ACID tables during Hive External replication**

With this bug fix, Hive tables will be filtered out of replication. Specifically, if the table is specified by a REGEX, the REGEX filter only applies to (matches) non-managed tables. If the table is not a REGEX and refers to a managed table, an error will occur.

**Cloudera Bug: OPSAPS-61656: Service monitor leaking Truststore reloader threads**

Fixed an issue where the Service Monitor leaks Truststore reloader threads when the Atlas Server Canary is enabled.



**Cloudera Bug: OPSAPS-61803: Remove Jetty version from error page for additional security**

Removed the "Powered by Jetty" message displayed by the Cloudera Manager Event Server's Jetty error page for additional security.

**Cloudera Bug: OPSAPS-61834: HBase replication not working with CDH 5**

The following syntax error would occur when creating an HBase policy if the source HBase was CDH 5:

```
NameError: uninitialized constant STATE const_missing at org/jruby/RubyModule.java:2647 (root) at /tmp/tmp.DFQlVU7GhI:1 load at org/jruby/RubyKernel.java:1087 (root) at /opt/app/cloudera/parcels/CDH-5.16.2-1.cdh5.16.2.p0.8/lib/hbase/bin/hirb.rb:177'
```

This has been fixed now to generate a different add-peer syntax if the source HBase is running on CDH 5.

**Cloudera Bug: OPSAPS-61835: Improve handling of empty command arguments**

Corruption of the arguments of one command in the Cloudera Manager database would prevent all running and future commands from progressing. Now, the corrupted command errors out if necessary, instead of being retried, and other commands are not affected.

**Cloudera Bug: OPSAPS-61846: Restrict krb5.conf path only when managed by Cloudera Manager**

Prior to this fix, when upgrading Cloudera Manager, in situations where a custom path for krb5.conf is set via Advanced Configuration Snippets, Cloudera Manager would return an error in the Cloudera Manager Admin Console and cause the upgrade to fail. The workaround was to set the krb5.conf path to either /etc/krb5.conf or any path under /etc/hadoop.

Going forward, when Cloudera Manager manages the Kerberos configuration file location i.e. "Manage krb5.conf through Cloudera Manager" setting is enabled, the expected paths for the file are either at /etc/krb5.conf or any path under /etc/hadoop. When this setting is not enabled, the user can set any path for the krb5.conf file.

**Cloudera Bug: OPSAPS-61905: Cloudera Runtime 7.1.7 compatible topology.py is not Python 3 compatible**

Spark jobs being run in a Python 3 environment will not be able to run due to a topology.py file that is not compatible with Python 3. The error logged by the failing Spark job is similar to the following:

```
--- 21/11/19 16:20:50 WARN net.ScriptBasedMapping: Exception running /etc/hadoop/conf.cloudera.yarn/topology.py 10.164.155.57 ExitCodeException exitCode=1: File ""/etc/hadoop/conf.cloudera.yarn/topology.py"", line 60 print rack ^ SyntaxError: Missing parentheses in call to 'print'. Did you mean print(rack)?
```

This problem will manifest if Cloudera Manager 7.4.4 is managing a cluster running Cloudera Runtime 7.1.7 or later, and the user attempts to launch a Spark job. The topology.py file has been updated to be compatible with python3. After upgrading to Cloudera Manager 7.6.1, restart the Spark service.

**Cloudera Bug: OPSAPS-61939: Cloudera Manager agent fails to clean up stale client configurations**

Fixed a bug where the Cloudera Manager agent failed to clean up directories under /var/run/cloudera-scm-agent/process/ccdeploy\*

**Cloudera Bug: OPSAPS-61965: Fix SAML SSO - VelocityEngine runtime failure**

Fixed an issue where a user gets the following error when logging in to Cloudera Manager when using SAML SSO:

```
org.apache.velocity.exception.ResourceNotFoundException: Unable to find resource '/templates/saml2-post-binding.vm'
```

**Cloudera Bug: OPSAPS-61972: HBase policy delete should clean up the policy details from a single peer**

When deleting an HBase Replication policy, the table Column Families are removed from the HBase peer. When last policy is deleted, the HBase peer is also deleted.

**Cloudera Bug: OPSAPS-62087: Upgrade ttorrent-core**

The ttorrent-core dependency was removed due to CVE issues CVE-2008-0071, CVE-2008-0364, CVE-2008-4434, CVE-2008-7166, CVE-2014-8515, CVE-2015-5474

**Cloudera Bug: OPSAPS-62296: Fix label for Knox Gateway UI link**

There has been an issue where the "Knox Gateway UI" link from the service page of a service with Knox SSO enabled. The Cloudera Manager Admin Console was incorrectly opening the Knox service page in the Cloudera Manager Admin Console. The link now opens the Knox Gateway UI as expected.

**Cloudera Bug: OPSAPS-62357: Atlas JDK 11 version check needs to be fixed**

Atlas JDK version check has now been improved to check for JDK 11. After upgrading Cloudera Manager, configuration staleness for Atlas service is expected, users must ensure sufficient downtime and restart Atlas service.

**Cloudera Bug: OPSAPS-62559: Delete Credentials is failing on RedHat8.2 with Active Directory KDC**

On RedHat 8 and later, you may encounter an error when attempting to delete credentials if Active Directory is used as the Kerberos KDC. This has been fixed.

**Cloudera Bug: OPSAPS-62581: Address CVE-2021-44228**

[CVE-2021-44228](#) has been addressed for log4j issues.

**Cloudera Bug: OPSAPS-62708: API REST GET /externalUserMappings/{uuid} no results - ENGESC-11872**

Fixed an issue where the Cloudera Manager API is throwing an HTTP 500 error due to a NullPointerException from the ExternalUserMappingManagerDaoImpl.getExternalUserMapping(uuid) method because the entity manager object is null.

**Cloudera Bug: OPSAPS-62711: Support Ldap auth for cancelQueryAPI in 7.1.7 SP1**

Impala queries cannot be canceled from the Cloudera Manager Admin Console or the impalaQueries API on a non-kerberized cluster if Cloudera Manager/impalad LDAP authentication is enabled. This fixes the issue by adding support for LDAP auth for cancelQueryAPI. Additionally, The administrator will need to add an LDAP username and password to the Cloudera Manager Impala configuration.

**Cloudera Bug: OPSAPS-62812: HostMonitor Missing HSTS Header**

Fixed an issue where the Service Monitor and Host Monitor only open a single port when TLS is used for increased security.

**Cloudera Bug: OPSAPS-62843: Multiple stats by different engines cause Hive 3 external replication to fail**

With this fix, Hive table column stats will now be correctly replicated between a CDP Private Cloud Base source cluster to a CDP Private Cloud Base destination cluster. With the above fix, administrators should not set the HIVE\_REPL\_STATS\_ENGINE parameter in the Hive Replication Environment Advanced Configuration Snippet (Safety Valve)".

**Cloudera Bug: OPSAPS-62976: HBase REST server does not catch its JVM properties from Cloudera Manager.**

Fixed a typo in the hbase.sh script that prevented catching up on changes from the configuration of the HBase REST service.

**Cloudera Bug: OPSAPS-63056, OPSAPS-63057: Add custom kerberos path to HADOOP\_OPTS**

When modifying the default path of the krb5.conf file in Cloudera Manager, the following issues were occurring:

- The credential generation for roles are failing

- KDC authentication with the Cloudera Manager server fails
- Services are failing to authenticate with the Cloudera Manager agent once manually getting services up by applying hacks (i.e adding relevant JVM arguments or env variables)
- Some services like HDFS, Livy, HiveServer and Knox are failing as they are unable to locate the new Kerberos path.

The above issues are fixed. For more information see this [Knowledge Base article](#).

## Known Issues in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1)

Known issues in Cloudera Manager 7.6.1

**Cloudera bug: 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***]
```

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

Bad Message 431 reason: Request Header Fields Too Large

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-61825: Refreshing the cluster using the Refresh Cluster option fails with an error.**

You may see the following error if you try to refresh your cluster from Cloudera Manager UI using the Refresh Cluster option:

```
com.cloudera.cmf.command.CmdExecException: com.cloudera.cmf.serv
ice.CommandException: No command 'UpdateSolrConfigSet' found for
role 'DbRole{id=21, name=RANGER-RANGER_ADMIN-1, hostName=xxxxxx-
xxxxxx-1.xxxxxx-xxxxxx.root.hwx.site}'
```

Avoid using the cluster-level Refresh Cluster command from Cloudera Manager. Instead, use the role-level Refresh command for the individual roles available in the services from the Actions dropdown menu.

**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.

### Technical Service Bulletins

#### TSB 2022-571: Increased heap memory in Reports Manager in Cloudera Manager 7.4.3+

“Directory Usage report should include a column that shows usage including Hadoop Distributed File System (HDFS) Snapshots” feature caused an unexpected increase of memory consumption in Reports Manager. Using the affected versions can cause heavy Java Virtual Machine (JVM) Pauses in the Reports Manager. Due to the JVM Pauses the HDFS Usage Reports cannot be updated.

#### Components Affected:

- Reports Manager

#### Products Impacted:

- Cloudera Data Platform (CDP) Private Cloud Base

#### Releases Impacted:

- CDP Private Cloud Base 7.1.7
- CDP Private Cloud Base 7.1.7 Service (SP) 1

#### Users Impacted:

- Users who actively use Reports Manager and the HDFS Usage Reports

#### Action required

- Request for a hotfix
- Alternatively, increase the heap size of the Reports Manager (`headlamp_heapsize`) at the following location: Cloudera Management Service > Configuration > `headlamp_heapsize`.

The recommended value is up to four times the current recommendation ( $4 * \text{FsImage size} + 2 \text{ Gb}$ ).

#### For example:

FsImage size: 20 Gb;

Current recommendation in the official documentation:  $4 * 20 \text{ Gb} + 2 \text{ Gb} = 82 \text{ Gb}$ ;

Recommended value for the increased heap memory needs:  $x * 82 \text{ Gb}$  ( $1 < x \leq 4$ )

#### Knowledge article

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

[Cloudera Customer Advisory: Increased heap memory in Reports Manager in Cloudera Manager 7.4.3+](#)

**TSB 2022-597: Cloudera Manager Event server does not clean up old events**

The Event Server in Cloudera Manager (CM) does not clean up old events from its index, which can fill up the disk. This leads to wrong “Event Store Size” health checks.

**Component affected:**

- Event Server

**Products affected:**

- Cloudera Data Platform (CDP) Private Cloud Base
- CDP Public Cloud

**Releases affected:**

- CDP Public Cloud 7.2.14 (CM 7.6.0), and 7.2.15 (CM 7.6.2)
- CDP Private Cloud Base 7.1.7 Service Pack (SP) 1 (CM 7.6.1)

**Users affected:**

- Users who have Event Server running

**Impact:**

- Event Server’s index fills up the space on the used disk eventually.

**Action required**

Patch: Please contact support for a patch to address this issue.

- **Workaround**

**Suggested workaround instructions:**

1. Stop the Event Server.
2. Check path for Event Server's index [eventserver\_index\_dir] in Cloudera Manager.
3. Archive /v4 folder in this path\*.

- a. Compress the v4 folder using the following command:

```
tar -czvf event_archive.tar.gz ${eventserver_index_dir}/v4
```

- b. Copy the archived version to an external disk.
  - c. Remove the \${eventserver\_index\_dir}/v4 folder.
4. Start the Event Server\*\*.

\*The archived version can be restored, by archiving the current index as described above, and extracting the archived version with the following steps:

- a. Stop the Event Server.
- b. Copy event\_archive.tar.gz to \${eventserver\_index\_dir}.
- c. Extract event\_archive.tar.gz using

```
tar -xvf event_archive.tar.gz
```

The extracted v4 folder should be under \${eventserver\_index\_dir}.

- d. Start the Event Server.\*\*\*

\*\* After the Event Server is restarted a new index is built, which cannot be merged with the previously archived index, if that is being restored.

\*\*\* After the archived index is restored, the Event Server will continue to build that index with the new events.

5. Delete the Event Server's index which is under /var/lib/cloudera-scm-eventserver/v4 by default, can be changed using eventserver\_index\_dir parameter which is without the v4 subfolder.
6. Restart the Event Server.

**Monitoring:**

- CM by default has thresholds to monitor the Event Server space using [eventserver\_index\_directory\_free\_space\_percentage\_thresholds] parameter.

You can adjust these as well by following the [Cloudera Manager documentation](#).

**Knowledge article**

For the latest update on this issue see the corresponding Knowledge article: [TSB 2022-597: Cloudera Manager Event server does not clean up old events](#)

## Documentation Errata in Cloudera Manager 7.6.1 (CDP Private Cloud Base 7.1.7 SP1)



**Important:** Do not upgrade to Cloudera Manager 7.6.1 if you are running CDP Private Cloud Data Services in your deployment.

**Cloudera Manager 7.6.1 now provides better support for NFS mounts**

Cloudera Manager 7.6.1 introduces the use of the `rpcinfo` command which is usually distributed as part of the `rpcbind` package to identify NFS (Network File System) mounts. You can verify the usage of NFS using the `findmnt` command or any similar tools and looking for a file system type of NFS.

**Track swap rate vs. total swap used**

Added a new health test that tracks swap rate, to reveal information that swap usage alone does not convey. The health test can be enabled by configuring Swap Memory Rate Thresholds.

**Cloudera Bug: OPSAPS-60517: Support metrics collection from secure endpoints**

Custom Service Descriptors can specify that the Cloudera Manager Agent host certificate is to be used for the purpose of TLS client verification when collecting metrics. Existing Custom Service Descriptors are unaffected by the change.

**Cloudera Bug: OPSAPS-61605: New validations for Hive 3 replication**

This modification is a CDH version check for Hive ACID tables during Hive External replication. If CDH version is 7 or above, the following will occur:

Hive tables will be filtered out of replication. Specifically, if the table is specified by a REGEX, the REGEX filter only applies to (matches) non-managed tables. If the table is not a REGEX and refers to a managed table, an error will occur.

**Cloudera Bug: OPSAPS-61773: Create only one HBase peer per source-destination cluster pair**

When a HBase replication is configured between a unique source and target, a single HBase replication peer will be created. Even when multiple RMAApp policies are created between a unique source and target, only one HBase replication peer will be created. Previously, each RMAApp policy created a separate HBase replication peer.

**Cloudera Bug: OPSAPS-61881: Cloudera Manager table data now included in Diagnostic Bundles**

Cloudera Manager now collects a critical set of table data from its own database as part of the Diagnostic bundle. For information on configuring this feature, see [Configuring collection of Cloudera Manager table data](#)

**Cloudera Bug: OPSAPS-61989: Upgrade activemq**

active-mq has been upgraded to the latest version.

**Cloudera Bug: OPSAPS-62295: Support for PostgreSQL 14**

Cloudera Manager is now compatible with the PostgreSQL 14 database.

**Support for MariaDB 10.5**

Cloudera Manager is now compatible with the MariaDB 10.5 database.

**Cloudera Bug: OPSAPS-62673: Support token API**

Two new APIs have been introduced for customers to retrieve a token key that will allow Cloudera to more accurately track assets, usage and node-counts, particularly in the absence of a diagnostic bundle. Customers provide the token to the support team when asked when creating a support case. To retrieve the token key, call:

```
GET /cm/clusterSupportTokens GET /clusters/{clusterName}/clusterSupportToken
```

You can also call this from the Cloudera Manager Admin Console. Go to Support Support Tokens.

**Cloudera Bug: OPSAPS-62675: Cluster support token available in the Cloudera Manager Admin Console**

Cloudera Manager can supply a "Cluster Support Token" through the Cloudera Manager Admin Console. This token may be requested by the Cloudera Support Portal when opening support cases. This feature is accessible to users who have global authority to view cluster information. For more information, see [Cluster Support Tokens using Cloudera Manager](#).

**Cloudera Bug: OPSAPS-62748: Cloudera Manager: Upgrade Logredactor to version 2.0.13**

Cloudera Manager is updated to use logredactor 2.0.13 for all releases.

**Cloudera Bug: OPSAPS-61220 New configuration properties for Server work directory path for Ranger services**

Ranger Admin / KMS / KMS-KTS server work directory can now be configured through the parameter `{{ranger.tomcat.work.dir}}`

Ranger RMS server work directory can now be configured through the parameter `{{ranger-rms.tomcat.work.dir}}`

Ranger Raz server work directory can now be configured through the parameter `{{ranger.raz.tomcat.work.dir}}`

### **Cloudera Bug: OPSAPS-61876: NiFi service in Diagnostic Bundles**

The NiFi service is now included in diagnostic bundle collection.

## **Cumulative hotfixes**

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.6.1 release.

### **Cloudera Manager 7.6.1 Cumulative hotfix 9**

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 9.

This cumulative hotfix was released on January 31, 2023.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF9 (version: 7.6.1-37037599):**

#### **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-62886: Replication Policies page takes a longer time to load when the replication policy count is high**

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-65562**

Enabling HBase snapshot export to Azure storage during HBase replication from CDH5 source cluster.

#### **NAV-7374: In solrconfig.xml configuration file, the embedded Solr's formdataUploadLimitInKB attribute must be increased from default 2 MB**

Updated the embedded Solr's `formdataUploadLimitInKB` attribute to 16 MB, as previously this limit is frequently reached in Navigator Metadata Server, in case of API calls used to mass update embedded Solr entities (For example, Nav2Atlas export, Navigator Metadata purge, queries for large amount of entities, etc).

#### **NAV-7350: Upgrade CXF library**

Upgraded CXF library to version 3.4.5

The repositories for Cloudera Manager 7.6.1-CHF9 are listed in the following table:



**Table 14: Cloudera Manager 7.6.1-CHF9**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@archive.cloudera.com/p/cm7/patch/7.6.1-37037599/ubuntu1604/apt/cloudera-manager.list</pre>

## Cloudera Manager 7.6.1 Cumulative hotfix 8

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 8.

This cumulative hotfix was released on August 10, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF8 (version: 7.6.1-30444079):**  
**OPSAPS-64325: Hue Load Balancer issues**

Earlier, the users were routed to a new Hue server only after they logged out. This resulted in less than optimal utilization of the newly added Hue servers. This issue has been resolved by adding a new configuration called Hue Load Balancer Cookie Refresh in Cloudera Manager. When you select this option, the Hue Load Balancer is configured to generate a new ROUTEID cookie value when you restart the Hue Load Balancer instance. This enables the Load Balancer to redistribute users across the Hue servers upon restart. For more information, see [Configuring high availability for Hue](#).

**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.

**OPSAPS-64187: Cloudera Manager Event Server does not clean up old events**

Fixed an issue where an Event Server cleanup did not work and was unable to clean the old events.

**OPSAPS-64020**

Upgraded spring-framework to 5.3.20.

The repositories for Cloudera Manager 7.6.1-CHF8 are listed in the following table:

**Table 15: Cloudera Manager 7.6.1-CHF8**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/27e78ad6/patch-5521/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF8 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 7

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 7.

This cumulative hotfix was released on June 30, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF7 (version: 7.6.1-28822345):**  
**OPSAPS-62471: Revert OPSAPS-32569 Disable HBase replication monitoring when Kerberos is enabled**

Fixed an issue where HBase replication monitoring was not enabled when Kerberos was enabled.

**OPSAPS-62007: When Auto-TLS is enabled then the value of the trustStorePath is overridden by the autogenerated truststore**

Previously when enabling Auto-TLS, it overwrote truststore paths (but not the corresponding passwords) for even those components where customer already set up TLS manually, which was not a expected behavior. This issue is now fixed, and the truststore paths of manual TLS components are kept intact.

**OPSAPS-60430: Kudu Ranger service repositories are not automatically created in medium duty DataHub clusters**

Kudu service in Ranger is now automatically created when multiple on Ranger HA setup.

The repositories for Cloudera Manager 7.6.1-CHF7 are listed in the following table:

**Table 16: Cloudera Manager 7.6.1-CHF7**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/b2fe9a6c/patch-5488/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF7 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 6

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 6.

This cumulative hotfix was released on June 07, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF6 (version: 7.6.1-27862530):**  
**OPSAPS-63759: Optional direct delete in DistCp snapshot-diff based replication**

When the accumulated temporary file count in a HDFS temporary folder (snapshot diff-based HDFS replication synchronizes the deletes and renames through a temporary directory on the target cluster) crosses the HDFS directory entry count limit per directory of ~6.4 items, the incremental replication fails and the replication process falls back to bootstrap replication (that is, all the files are replicated).

OPSAPS-63759 introduces an optional direct delete behavior where delete operations are run directly without the intermediate moves into the common temporary directory. To enable this workaround:

1. Go to the target Cloudera Manager Clusters *HDFS service* Configuration tab.
2. Search for the Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml property.
3. Add the com.cloudera.enterprise.distcp.direct-rename-and-delete.enabled=true key-value pair.

This parameter activates the direct delete approach.

Optionally, you can set the com.cloudera.enterprise.distcp.direct-delete.log-interval=[\*\*\*enter a value (n) greater than 0\*\*\*] key-value pair to override the default (100000) delete count for each delete progress log message.



**Note:** If you update these parameters after the HDFS file limit per directory is crossed, the next replication policy run is a bootstrap operation (that is, all the files are replicated and snapshot-diffs are not used). Snapshot diffs (or incremental replication) are used only after a successful bootstrap run. Note that the activation of this workaround can be followed in the logs printed by DistCp.

The repositories for Cloudera Manager 7.6.1-CHF6 are listed in the following table:

**Table 17: Cloudera Manager 7.6.1-CHF6**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat8/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat7/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat6/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/sles12/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/sles12/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
Ubuntu 20	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/5c5dbed8/patch-5451/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF6 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 5

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 5.

This cumulative hotfix was released on May 23, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF5 (version: 7.6.1-27218580):**  
**OPSAPS-63605: An Event Server cannot start after an upgrade due to a field type mismatch**

Fixed an issue where, in case of sufficiently long event attributes, a deprecated field type is replaced with an incompatible field type in the backing data store as part of the Cloudera Manager upgrade. This prevents the Event Server from starting. This fix changes the field type to a compatible one.

The repositories for Cloudera Manager 7.6.1-CHF5 are listed in the following table:



**Table 18: Cloudera Manager 7.6.1-CHF5**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/fab4e884/patch-5448/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF5 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 4

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 4.

This cumulative hotfix was released on May 11, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF4 (version: 7.6.1-26665959):**

**OPSAPS-24898: Users are having trouble in reading SNMP traps sent by Alert Publisher as the SNMP traps does not have all varbinds**

To fix this issue, add `snmp.omit.null=false` when using Alert Publisher's Alert Publisher Advanced Configuration Snippet (Safety Valve) for `alertpublisher.conf` parameter, and restart Alert Publisher. After that Alert Publisher sends all defined varbinds in all SNMP traps. NULL is used, when the varbind has no value.

The repositories for Cloudera Manager 7.6.1-CHF4 are listed in the following table:

**Table 19: Cloudera Manager 7.6.1-CHF4**

Repository Type	Repository Location
RHEL 8 Compatible	Repository: <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat8/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat8/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu1804/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu1804/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 16	Repository:  <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu1604/apt</pre> Repository file:  <pre>https://username:password@bits.cloudera.com/035f2efa/patch-5433/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF4 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 3

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 3.

This cumulative hotfix was released on April 29, 2022.



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

The repositories for Cloudera Manager 7.6.1-CHF3 are listed in the following table:

**Table 20: Cloudera Manager 7.6.1-CHF3**

Repository Type	Repository Location
RHEL 8 Compatible	Repository:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat8/yum</pre> Repository File:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	Repository:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat7/yum</pre> Repository File:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	Repository:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat6/yum</pre> Repository File:  <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/redhat6/yum/cloudera-manager.repo</pre>

Repository Type	Repository Location
SLES 12	Repository: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/sles12/yum</pre> Repository File: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	Repository: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu2004/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu2004/apt/cloudera-manager.list</pre>
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/ee3b63f8/patch-5429/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF3 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 2

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 2.

This cumulative hotfix was released on April 13, 2022.



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

**Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF2 (version: 7.6.1-25197139): OPSAPS-58664: Hive LDAP properties pushed to hive-site.xml**

After setting LDAP properties in Hive on Tez service, the configurations are not pushed into the hive-site.xml for Hive on Tez service even after a restart. This issue is fixed now.

The repositories for Cloudera Manager 7.6.1-CHF2 are listed in the following table:

**Table 21: Cloudera Manager 7.6.1-CHF2**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu2004/apt/cloudera-manager.list</pre>

Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/eadd4464/patch-5407/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF2 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.6.1 Cumulative hotfix 1

Know more about the Cloudera Manager 7.6.1 cumulative hotfixes 1.

This cumulative hotfix was released on April 07, 2022.



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

### Following are the list of fixes that were shipped for Cloudera Manager 7.6.1 CHF1 (version: 7.6.1-24871424): OPSAPS-63077: Decommissioning/recommissioning nodemanager failure in YARN

If Zookeeper configuration store is set in YARN and QueueManager is not used, then every YARN node decommission causes an exception, because it calls the `refreshQueues` command (which is not allowed if a mutable configuration store is used). This issue is fixed now.

### OPSAPS-63124: Enabling snapshot processing causes huge memory consumption in the Reports Manager

Enabling snapshot processing causes an unexpected increase of memory consumption in the Reports Manager. This issue is fixed now by turning off this feature by default, therefore there is no increase in memory consumption as much as before. For users who want to use the Enable snapshot processing feature to view the snapshot space consumption in the HDFS Directory Usage Report, can enable this feature at Reports Manager configuration page with the `snapshot.processing.enabled` switch.

### OPSAPS-63419: Yarn MR Aggregation job fails with pt\_PT locale

Fixed an issue where the Yarn MR Aggregation job got stuck with certain locale settings.

The repositories for Cloudera Manager 7.6.1-CHF1 are listed in the following table:

**Table 22: Cloudera Manager 7.6.1-CHF1**

Repository Type	Repository Location
RHEL 8 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat8/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat8/yum/cloudera-manager.repo</pre>
RHEL 7 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat7/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat7/yum/cloudera-manager.repo</pre>
RHEL 6 Compatible	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat6/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/redhat6/yum/cloudera-manager.repo</pre>
SLES 12	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/sles12/yum</pre> <p>Repository File:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/sles12/yum/cloudera-manager.repo</pre>
Ubuntu 20	<p>Repository:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu2004/apt</pre> <p>Repository file:</p> <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu2004/apt/cloudera-manager.list</pre>



Repository Type	Repository Location
Ubuntu 18	Repository: <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu1804/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu1804/apt/cloudera-manager.list</pre>
Ubuntu 16	Repository: <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu1604/apt</pre> Repository file: <pre>https://username:password@bits.cloudera.com/b0432c4a/patch-5396/ubuntu1604/apt/cloudera-manager.list</pre>



**Note:** In Cloudera Manager 7.6.1 CHF1 release, you cannot use your regular payroll credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

## Cloudera Manager 7.4.4 Release Notes

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



**Important:** Cloudera Manager has been replaced with the 7.4.4-24429768 hotfix release that contains PATCH-5393 that includes a fix for the issue described in the [TSB-545 Critical vulnerability in log4j CVE-2021-44228](#).

## What's New in Cloudera Manager 7.4.4

New features and changed behavior for Cloudera Manager 7.4.4.

### Upgrades from CDH 6 to CDP are now supported.

You can upgrade from CDH 6.1 or higher to CDP Private Cloud Base. See [In-place upgrade from CDH 6 to CDP Private Cloud Base](#).

### New Support for Dell OneFS (Isilon)

The following upgrades are now supported for Dell EMC PowerScale OneFS:

- CDH 5 to CDP Private Cloud Base 7.1.7
- HDP 2 to CDP Private Cloud Base 7.1.7

New installations on Dell OneFS are now supported for CDP Private Cloud Base 7.1.7.

### New Upgrade Guide Companion app

We are introducing a companion to the already existing [Upgrade Guide](#) we currently publish with all releases. The Upgrade Companion is a stand-alone web page that is hosted as part of [docs.cloudera.com](#) but is separate from the rest of the product documentation. It will provide a central hub for all activities related to upgrading our products regardless of the form factor. The Upgrade Companion will provide a set of content tabs that cover the major points of a customer's upgrade journey:

- Getting Started
- Pre-upgrade Tasks
- Upgrade the Cluster
- Post-upgrade Tasks
- Troubleshooting

Each tab includes content and links that help the user navigate that particular step in the journey. In addition, the Upgrade Companion will also include a full set of filters that are used to filter content based on specific configurations selected.

See [Upgrade Guide Companion](#).

### **New supported operating systems**

The following operating systems are now supported for use with CDP Private Cloud Base 7.1.7:

- RHEL 8.2
- Ubuntu 20

### **increase replication policies page refresh rate greater than 15sec**

The auto-refresh interval on the Replication and Snapshots pages has been increased from 15 seconds to 2 minutes. A refresh button has been added to allow more frequent refreshes if desired;

### **New supported databases**

The following databases are now supported for use with CDP Private Cloud Base 7.1.7:

- MariaDB 10.3 and 10.4
- Oracle 19.9

### **Rollback of upgrades to CDP**

Rollback is now supported for the following upgrades:

- HDP 3 to CDP 7.1.7 (Cloudera Manager 7.4.4) or higher. See [Rollback HDP Services from CDP 7.1.7](#)
- CDH 6 to CDP 7.1.7 (Cloudera Manager 7.4.4) or higher. See [Rolling back a CDH 6 to CDP Private Cloud Base upgrade](#) for the procedures.

### **Add test LDAP Configuration feature in Cloudera Manager**

The configured LDAP settings can now be tested through the Cloudera Manager Admin Console or API. After saving, LDAP settings can be tested without restarting the Cloudera Manager server. This is available in the Cloudera Manager Admin Console under Administration -> Users & Roles -> LDAP/PAM Groups and in the API at /cm/commands/testExternalAuthentication.

### **Cloudera Manager agent to support static UID+GID generation natively**

Cloudera Manager now allocates fixed numeric IDs for service user accounts and service group accounts (for example, the HDFS service runs in the "hdfs" user account).

Previously, Cloudera Manager allowed the OS on each host to choose the numeric ID underlying the service accounts (for example, service user account "hdfs" would be allocated numeric ID 986). This resulted in different hosts having random assignments of numeric IDs, which would make it problematic to move partitions between hosts.

With this release, Cloudera Manager statically allocates numeric IDs when a new host is added to Cloudera Manager. For services in the CDP parcels, the numeric ID will come from a static list. For services in other parcels, the numeric ID is chosen by hashing the service name.

If a service user account or group account already exists, Cloudera Manager will not change the numeric ID. Therefore existing hosts will not be changed. If customers were previously depending on the semi-random allocation of numeric IDs to match between hosts, this change will cause new hosts to have a different (though static) allocation from previously added hosts.

If customers pre-allocate service user and group accounts for the Cloudera Manager managed services, Cloudera Manager will not modify those accounts.

The feature is turned on by default. To disable it, customers should set the property `is_static_uid_gid_enabled` to false in `/etc/cloudera-scm-agent/config.ini` on all cluster hosts.

#### **New configuration property for Streams Messaging Manager CSD**

The property `prometheus.query.threads` determines how many parallel requests Streams Messaging Manager should send to Prometheus when fetching metrics (in case Prometheus is used as a backend metrics store). This value should match the value of the `query.max-concurrency` property in Prometheus. The default value for both is 20.0.

#### **New Date Format for killed Java process message**

When a Java process is killed due to exceeding memory resources (Out of Memory - OOM), Cloudera Manager creates a file called `killed_by_killparent_on_oom` in the process directory. The timestamp stored in that file has been updated to use ISO 8601 format.

#### **Make the YARN/HDFS SSL/TLS Cipher Suite's value dependent on FIPS compliant mode**

For FIPS compliant clusters, the SSL/TLS Cipher Suite should be set to Intermediate 2018 in order to be able to access the web UIs of the services. Hive, HBase, HDFS and YARN already use Intermediate 2018 as the default for FIPS mode.

#### **Changing `stacks_collection_directory` will also set ownership of the directory to the process user**

Cloudera Manager now displays a warning message when users try to set the "Stacks Collection Directory/ Heap Dump Directory" to non-recommended paths. Previously, the operation of setting "Stacks Collection Directory/ Heap Dump Directory" could change the ownership of any system directory. Also, sharing the same directory among multiple service roles caused an ownership race. Thus, any process that tries to access the folder might be denied and fail to start.

With this release, Cloudera Manager guides the user to set those paths under `/tmp` and `/var/log`. (For example: `/tmp/hdfs_stacks_collection_dirs`). If this rule is contradictory to a previous deployment, you can suppress or ignore the warning message.

#### **Cloudera Manager now configures Atlas Hooks for Sqoop**

Cloudera Manager is now capable of enabling and configuring the Sqoop Atlas Hook. See: <http://atlas.apache.org/2.0.0/Hook-Sqoop.html>. The configuration happens automatically, no extra, manual configuration is required from the users. Cloudera Manager will configure the Hook in `sqoop-site.xml` and it will automatically generate the `atlas-application.properties` file for Sqoop. If you are installing a fresh cluster with Atlas being present, then the Hook will be enabled automatically and the `atlas-application.properties` will be generated for Sqoop. If you are upgrading from an older cluster then you need to enable the Hook manually. To enable Hook manually:

1. Go to the configuration page for the Sqoop service.
2. Search for "Atlas".
3. Enable the checkbox and then re-deploy the client configurations using Cloudera Manager.

#### **: Add new auth-to-local rule for Atlas**

Support has been added for adding an auth-to-local rule for Atlas principal to Atlas service user mapping.

#### **Improved start up performance of YARN and MapReduce jobs.**

Workload setup for YARN, MapReduce is now about 20% faster.

Cloudera Manager changed `topology.map` file generation from XML to INI format to improve the performance of the script `topology.py`. `topology.py` has been modified to process `topology.map` in INI format.

#### **IBM Power PC (PPC) is supported with CDP Private Cloud Base 7.1.7 on RHEL 7 and RHEL 8**

IBM PowerPC is supported with the following operating systems:

- RHEL 7.9

- RHEL 8.2

Please see [Known Issues for IBM PowerPC](#) on page 72.

## Fixed Issues in Cloudera Manager 7.4.4

Fixed issues in Cloudera Manager 7.4.4

**Cloudera Bug: OPSAPS-48387: Host Inspector incorrectly reports 5.x version for supervisord**

Host Inspector no longer shows Cloudera Manager version attached to supervisord version.

**Cloudera Bug: OPSAPS-49267: Bundle log times are truncated early**

Fixed an issue where Cloudera Manager diagnostic bundle collection fails to collect role logs for the specified time range.

**Cloudera Bug: OPSAPS-54051: Metric names are not consistent in metric filter**

Fixed an issue where an invalid metric name was reported when adding some metrics to custom metric filter lists. These metrics can now be added to filter lists using their names as they appear in charts. Already configured filter lists are unaffected.

**Cloudera Bug: OPSAPS-55159: BDR job produced misleading message about snapshottable dir detection**

Fixed the misleading warning message.

**Cloudera Bug: OPSAPS-59818: Support for snapshot policy name containing "/" symbols**

You must ensure that the snapshot policy name does not contain the characters % . ; / \ nor any character that is not ASCII printable, which includes the ASCII characters less than 32 and the ASCII characters that are greater than or equal to 127.

**Cloudera Bug: OPSAPS-61078: Set kerberos ticket cache location for Omid**

Previously the Omid component was unable to refresh its Kerberos tickets, so after some time it failed to work properly and was unable to authenticate to HBase. This resulted transactional Phoenix queries to fail. This issue is now fixed and the Omid component can function correctly on kerberized clusters.

**Cloudera Bug: OPSAPS-61133: Disable GRPC TLS by default in Ozone**

Enabling GRPC TLS for Ozone caused issues starting the Cloudera Manager server in clusters upgraded to CDP Private Cloud Base 7.1.6 or 7.1.7. This setting is now disabled by default.

**Cloudera Bug: OPSAPS-58867: Cluster with custom kerberos principle deployment failing for Yarn's first run failure**

yarn.admin.acl values are now set according to the principal names.

**Cloudera Bug: OPSAPS-60022: add follow redirect -L in scm\_prepare\_node.sh - to fix issues with empty "baseurl" in .repo files**

Previously, Cloudera Manager failed to follow redirects of the repository URL provided for agent installation, causing agent installation to fail if a URL with a redirect was provided. Now, a repository URL with a redirect can be used successfully.

**Cloudera Bug: OPSAPS-60175: Internal error in Directory Usage Report**

Fixed the 'Internal error processing filesearch2' error in the Directory Usage Report when setting a HDFS quota in the Cloudera Manager Admin Console.

**Cloudera Bug: OPSAPS-60264: Create Ranger audit logs in HDFS for Schema Registry**

The ranger-audit configuration for Schema Registry did not contain an entry for defining where the audit files will be stored in HDFS. When xasecure.audit.destination.hdfs was set to true, this caused a silent failure in Ranger and no files would be written to HDFS. This issue has now been fixed and the audit files are being created on HDFS.

**Cloudera Bug: OPSAPS-60454: Cloudera Manager should add existing users to groups specified by a parcel**

Fixed an issue in which user-group mappings specified via parcel was not created properly if the service users already exist. Cloudera Manager now adds existing users to groups as appropriate.

## Known Issues in Cloudera Manager 7.4.4

Known issues in Cloudera Manager 7.4.4

**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***]
```

**OPSAPS-61022: Role logging process is getting stuck during Cloudera Manager Agent upgrade**

After you upgrade Cloudera Manager Agent, role logging process is stopped. Those roles that happen to log regularly will have their logging threads stuck, possibly causing the entire role to hang.

Restart the cluster after the Cloudera Manager Agent upgrade to restart the Role logging process.

**OPSAPS-60943 Clicking on Historical Disk Usage causes error**

On the Reports page in the Cloudera Manager Admin Console, clicking the link for Historical Disk Usage by (User or Group) causes the following error, caused by a Null Pointer Exception, to appear:

Server Error

A server error has occurred. The full stack trace is not shown here due to security reasons. See Cloudera Manager Server log for details.

Set the start and end times to a shorter time period by adjusting the following values in the URL:

```
&start=2021-11-09&end=2021-12-09
```

**OPSAPS-61905 Spark jobs will not be able to run due to topology.py file that is not compatible with python3.**

Manually edit topology.py file in the /etc/hadoop/conf\* directories. Fix python3 incompatible lines.

**Cloudera bug: 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
```

**CDPD-26099 Extra steps required to run Hue on RHEL 8**

See the following Hue administration topics:

- MySQL - [Installing and configuring MySQL on RHEL 8](#)
- MariaDB - [Installing and configuring MariaDB on RHEL 8](#)

**CDPD-28390 Rolling restart of HDFS JournalNodes may timeout on Ubuntu 20**

If the restart operation times out, you can manually stop and restart the NameNode and JournalNode services one by one.

**CDPD-27663 RPC TLS configuration for Ozone is supported only on new CDP 7.1.7 clusters**

Known Issue Description: gRPC TLS configuration for Ozone is supported only on new CDP 7.1.7 clusters and not on clusters upgraded from CDP 7.1.6 to CDP 7.1.7.

If you want to enable gRPC TLS on the upgraded CDP 7.1.7 clusters, you must contact Cloudera Support for more information.

**OPSAPS-59163 Client Configuration downloaded from Cloudera Manager Admin Console is not the same as client configuration downloaded to cluster hosts**

If you deploy the client configuration to a host that is not managed by Cloudera Manager, you will need to make the following change:

1. Unzip the client configuration bundle.
2. Edit the `hadoop-env.sh` file and change the line that begins with `export HADOOP_MAPRED_HOME=` to

```
export HADOOP_MAPRED_HOME=<path to Jar files>
```

**OPSAPS-59802 – Zeppelin and Livy roles should be co-located on the same host.**

When installing or upgrading to CDP Private Cloud Base, you must co-locate all Zeppelin and Livy roles on the same cluster host due to an issue with certificate generation.

**OPSAPS-60412 Extra step required when using Cloudera Manager Trial installer on Ubuntu 20**

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:

```
apt-get install libncursesw5
```

**OPSAPS-60721 Ozone fails to start when SCM High Availability is enabled**

The Ozone SCM Primordial Node ID is a required field that needs to be specified with one of the SCM hostnames during Ozone HA installation.

Ozone SCM can either be deployed in a 3 node or 1 node configuration. For the 1 node configuration, the Ozone SCM Primordial Node ID configuration property is not a required configuration. However for 3 nodes, this field is a required configuration to be added during initialization of SCM.

When adding the Ozone service, enter the hostname of one of the SCM host in the Ozone SCM Primordial Node ID field on the Review Changes page. If this value is not set, the startup of Ozone services will fail.

**OPSAPS-61045 Upgrading cluster with Hive requires Hue**

If you have upgraded a cluster to CDP 7.1.7 and the source cluster includes the Hive service and the Hue service is not included, the Hive Metastore may fail after the upgrade. Perform the following steps to restore the Hive Metastore:

1. Ensure that you add a Hue user before proceeding to add the required Ranger policies for the Hue user.
2. Log in to the Cloudera Manager Admin Console.
3. See if Health check issue is observed.
4. Navigate to Clusters
5. Select the Ranger service
6. Click Web UI. This redirects to the Ranger service page.
7. On the Ranger Admin UI, click Service Manager

## 8. Add the required Ranger policies for Hue user

The Policies include all - hiveservice, all - global, all - url, all - database, table, column and all - database,udf policies created under cl1\_hive. For more information, see Ranger policies for components.

After the Hue user is added to the policies metastore health check issue is no longer observed in the Cloudera Manager portal.

### OPSAPS-61278: The SRM Client's secure storage fails to generate correctly in FIPS-enabled clusters

In a FIPS enabled cluster, the SRM Client's secure storage fails to generate correctly. As a result, the automatically generated configuration used by the srm-control tool will contain unresolvable references, making it unusable.

There are two workarounds for this issue. Choose one of the following:

- Configure SRM using the Streams Replication Manager's Replication Configs Cloudera Manager property.

Ensure that all cluster connection related properties (cluster aliases, bootstrap servers, security-related properties) are added, with the appropriate prefixes, for all clusters taking part in the replication process.

- Manually create a custom configuration file and use it with the srm-control tool.
  1. Create a copy of the default configuration located at /etc/streams\_replication\_manager/conf/srm.properties.
  2. Update all security related properties in the copy with the appropriate values.

The values that you must update are similar to the following example:

```
${secure:/var/lib/streams_replication_manager/client.store:ext_ssl_truststore_password}
```

Ensure that you replace all \${...} references with actual values such as the key and truststore locations, passwords, and so on.

3. Run the srm-control tool using the --config option.

For example:

```
srm-control topics --config [***PATH TO CUSTOM CONFIGURATION FILE***] --source [***SOURCE_CLUSTER***] --target [***TARGET_CLUSTER***] --add [***TOPIC1***],[***TOPIC2***]
```

### OPSAPS-61523 Failure when installing Cloudera Manager Agents

When installing the Cloudera Manager Agent package on new hosts through either the Add Hosts wizard or Add Cluster wizard, if you select Cloudera Repository during the Select Repository step, the Agent Installation fails with message "Failed to Copy Installation Files".

Select Custom Repository instead and enter the URL and your license credentials in the following format:

```
https://[username]:[password]@archive.cloudera.com/p/cm7/7.4.4
```

## Technical Service Bulletins

### TSB 2022-571: Increased heap memory in Reports Manager in Cloudera Manager 7.4.3+

"Directory Usage report should include a column that shows usage including Hadoop Distributed File System (HDFS) Snapshots" feature caused an unexpected increase of memory consumption in Reports Manager. Using the affected versions can cause heavy Java Virtual Machine (JVM) Pauses in the Reports Manager. Due to the JVM Pauses the HDFS Usage Reports cannot be updated.

#### Components Affected:

- Reports Manager

**Products Impacted:**

- Cloudera Data Platform (CDP) Private Cloud Base

**Releases Impacted:**

- CDP Private Cloud Base 7.1.7
- CDP Private Cloud Base 7.1.7 Service (SP) 1

**Users Impacted:**

- Users who actively use Reports Manager and the HDFS Usage Reports

**Action required**

- Request for a hotfix
- Alternatively, increase the heap size of the Reports Manager (headlamp\_heapsize) at the following location: Cloudera Management Service > Configuration > headlamp\_heapsize.

The recommended value is up to four times the current recommendation (4 \* FsImage size + 2 Gb).

**For example:**

FsImage size: 20 Gb;

Current recommendation in the official documentation:  $4 * 20 \text{ Gb} + 2 \text{ Gb} = 82 \text{ Gb}$ ;

Recommended value for the increased heap memory needs:  $x * 82 \text{ Gb}$  ( $1 < x \leq 4$ )

**Knowledge article**

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

[Cloudera Customer Advisory: Increased heap memory in Reports Manager in Cloudera Manager 7.4.3+](#)

## Known Issues for IBM PowerPC

Known Issues for CDP Private Cloud Base 7.1.7 deployed on IBM PowerPC.

**Peer to peer Parcel distribution not working on IBM PowerPC on RHEL 8.2**

Peer to peer Parcel Distribution is not working on Redhat 8 PowerPC platforms. As such, parcel distribution will fail or get stuck when attempting to install Cloudera Runtime parcels. Before installing or upgrading Cloudera Runtime, use the following work-around to enable installation of Cloudera Runtime parcels.

1. Open the Cloudera Manager Admin Console.
2. Go to OPSAPS-61285HostsAll Hosts Configuration.
3. Locate the P2P Parcel Distribution Port property.
4. Change the value to 0.

If the parcel download and distribution has already failed, restart all of the Cloudera Manager agents.

**Open SSL 1.11g required for IBM PPC with RHEL 7**

In order to start the Hue service, OpenSSL 1.11g must be installed on all cluster hosts when installing CDP Private Cloud Base 7.1.7 on IBM PowerPC and RHEL 7.

**OPSAPS-61326 Hive Server fails to start on IBM PowerPC with RHEL 8**



When adding a cluster that includes the Hive service, the service may fail to start and the following error message displays:

```
[main]: MetaException(message:Failed to instantiate listener named: org.apache.kudu.hive.metastore.KuduMetastorePlugin, reason: java.lang.ClassNotFoundException: org.apache.kudu.hive.metastore.KuduMetastorePlugin)
```

If the Hive service fails to start, do the following:

1. Open the Cloudera Manager Admin Console.
2. Go to the Hive service.
3. Click the Configuration tab.
4. Change the following properties:

**Hive Metastore Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml**

Add the following:

```
<property>
  <name>hive.metastore.transactional.event.listeners</name>
  <value>
    org.apache.hive.hcatalog.listener.DbNotificationListener
  </value>
</property>
```

**HiveServer2 Advanced Configuration Snippet (Safety Valve) for hive-site.xml**

Add the following:

```
<property>
  <name>hive.metastore.transactional.event.listeners</name>
  <value>
    org.apache.hive.hcatalog.listener.DbNotificationListener
  </value>
</property>
```

5. Click Resume in the wizard to restart the installation wizard.

**CDPD-26099 Extra steps required to run Hue on RHEL 8**

See the following Hue administration topics:

- MySQL - [Installing and configuring MySQL on RHEL 8](#)
- MariaDB - [Installing and configuring MariaDB on RHEL 8](#)