Cloudera Manager 7.6.5

Release Notes

Date published: 2020-11-30
Date modified: 2022-05-25

CLOUDERA

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.6.5 Release Notes.....4
What's New in Cloudera Manager 7.6.5.....4
Fixed Issues in Cloudera Manager 7.6.5.....4
Known Issues in Cloudera Manager 7.6.5.....7

Cumulative hotfixes.....8
Cloudera Manager 7.6.5 Cumulative hotfix 1.....8
Cloudera Manager 7.6.5 Cumulative hotfix 2.....10
Cloudera Manager 7.6.5 Cumulative hotfix 3.....12
Cloudera Manager 7.6.5 Cumulative hotfix 4.....14
Cloudera Manager 7.6.5 Cumulative hotfix 5.....15

Cloudera Manager 7.6.5 Release Notes

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

What's New in Cloudera Manager 7.6.5

New features and changed behavior for Cloudera Manager 7.6.5.

Cloudera Bug: OPSAPS-62673 Support token API

We introduced two new APIs 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.

To retrieve the token key, use the following REST API call:

```
GET /cm/clusterSupportTokens GET /clusters/{clusterName}/cluster
SupportToken
```

Cloudera Bug: OPSAPS-62675 Cluster support token

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.

How to use: This feature is accessible to users who have global authority to view cluster information. In the Cloudera Manager Admin Console, click the "Support" item in the left menu bar, then select "Support Token". Cloudera Manager will then display a Support Token for each managed cluster. Then Support Token string can be copied and pasted or entered into the Cloudera Support Portal.

Fixed Issues in Cloudera Manager 7.6.5

Fixed issues in Cloudera Manager 7.6.5.

Cloudera Bug: OPSAPS-63460 :

NFS mounts in pods are preventing nodes from restarting for an upgrade. This happens due to Longhorn going into a repair mode, please wait for the repair to complete and then resume the upgrade.

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 thje Atlas service is expected, users must ensure sufficient downtime and restart the Atlas service.

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

For CDP Private Cloud Base running on RedHat 8 and higher, 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-63124: Add option for Reports Manager snapshot processing to be turned on/off

Enabling snapshot processing caused an unexpected increase of memory consumption of the Reports Manager. This fix turns off this feature by default, therefore the memory consumption will not increase as much as before. For customers who want to use the snapshot processing feature and see the snapshot space consumption in the HDFS Directory Usage Report, the feature can be enabled on the Reports Manager configuration page with the snapshot.processing.enabled property.

Cloudera Bug: OPSAPS-62167NFS provisioner fails on cluster with more than ~10 nodes

Fixed longhorn nfs_provisioner failing to start on clusters with more than 10 nodes.

Cloudera Bug: OPSAPS-62657: ECS HA fails during FirstRun

Fixed an issue where selecting multiple ECS Server hosts during install would randomly result in a installation failure.

Cloudera Bug: OPSAPS-61852: Unable to remove hosts from Cloudera Manager or cluster - non-existing host running Docker server previously

For more information, see Manually uninstalling ECS from a cluster

Cloudera Bug: OPSAPS-61278: The Streams Replication Manager Client's secure storage fails to generate correctly in FIPS-enabled clusters

The Streams Replication Manager client configuration secure storage did not work on FIPS-enabled clusters, which caused problems when trying to use the srm-control tool with the deployed client configurations. Secure storage is now working in FIPS enabled clusters.

Cloudera Bug: OPSAPS-62087: Upgrade ttorrent-core

The ttorrent-core dependency has been removed due to CVE issues. This fixes the following CVEs: CVE-2008-0071, CVE-2008-0364, CVE-2008-4434, CVE-2008-7166, CVE-2014-8515, CVE-2015-5474

Cloudera Bug: OPSAPS-62548: TopicMetrics get deleted from Cloudera Manager during restart or Kafka partition reassignment

Fixed an issue where KafkaTopicMetrics were accidentally deleted from ServiceMonitor's Timeseries database during a Kafka restart or partition leader change.

Cloudera Bug: OPSAPS-62581: Address log4j CVE-2021-44228

This patch addresses CVE-2021-44228 for log4j.

Cloudera Bug: OPSAPS-62588: Cloudera Manager: Upgrade Logredactor to version 2.0.11 to remediate CVE-2021-44228

This patch addresses CVE-2021-44228 affecting log4j library.

Cloudera Bug: OPSAPS-62670: Upgrade the transitive dependency of Log4j2 used by Hive in Cloudera Manager to 2.17.1

In some scenarios, a role may already exist in Ranger, In that case Authzmigrator tool throws an error because the role already exists. This has been fixed.

Cloudera Bug: OPSAPS-62760: Jetty version shown in HTTP header

The Jetty error page has been modified to hide the version and Jetty server name.

Cloudera Bug: OPSAPS-62770: Cloudera Manager Server setting HBaseCmdOpts.hbaseClusterKey incorrectly.

When using the Cloudera Manager API, when ApiHBaseReplicationArguments.hbaseClusterKey was left null/empty, the Cloudera Manager server supplied an incorrect default value for the cluster key. With this fix, if the value is null or empty, the correct cluster key is set.

The cluster key generated is hbase.zookeeper.quorum:hbase.zookeeper.property.clientPort:zookeeper.znode.parent.

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-62836: WAITING_FOR_SOURCE_RESTART status when cluster setup hasn't started

Sometimes during HBase Replication First Time setup, the status may report WAITING_FOR_SOURCE_RESTART before it is really waiting for the source to restart. This behavior has been fixed to report the correct status.

Cloudera Bug: OPSAPS-62910: HBase peer is not removed if several policies are deleted simultaneously

When attempting concurrent deletion of an HBase policy, when the last policy referencing the HBase peer is deleted, the HBase peer will be deleted as well.

Cloudera Bug: OPSAPS-62948: Simultaneous HBase policy creation can fail

When attempting to create multiple HBase policies concurrently, sometimes all of the create operations did not complete. With this fix, all concurrent create operations should succeed.

Cloudera Bug: OPSAPS-62956: Failed delete of policy for which creation failed

When multiple HBase policies are created concurrently, sometimes some of them would fail, or succeed but have wrong column families saved. With this fix, they should now all succeed, and the underlying HBase peer should contain all of the tables/column families from all the policies created.

Cloudera Bug: OPSAPS-62970: Upgrade AuthzMigrator to handle Ignore "already exists" failures

This fix handles the scenario where roles already exist in Ranger.

Cloudera Bug: OPSAPS-62980: Browser crashes with out-of-memory error when Dashboards contain numerous or complex charts

Browser crashed with out-of-memory error on complex Dashboard pages due to charts resize, drag and drop functionality.

You can now use the new Edit Layout menu option on the Dashboard pages and chart sections (e.g. Cluster, Host, Service, Role status pages) for enabling resize functionality. By default, the charts position and size are static. In order to modify the chart size, position they use the Edit Layout menu option.

Cloudera Bug: OPSAPS-62998: Synchronization of HBase peer disable/enable

When concurrent HBase enable/disable policy operations are run, sometimes the final policy status was inconsistent. For instance, after the last operation that completed, the policy status was not set as desired. This situation can be sporadic. With this fix, the HBase policy status will be set reliably.

Cloudera Bug: OPSAPS-63069: Kafka keystore and truststore type is not configured for Cruise Control metrics reporter

The keystore and truststore types are now correctly supported by the Cruise Control metrics reporter in the Kafka broker. Previously, the type would not be configured, causing issues if the store type did not match the default type. Now the type is correctly configured.

Cloudera Bug: OPSAPS-63077: Fix decommisioning/recommissioning nodemanager failure in YARN

If Zookeeper config store is set in YARN, and QueueManager is not used every YARN node decommission caused an exception, because it called the refreshQueues command (which is disallowed if a mutable configuration store is used). This has been fixed

Cloudera Bug: OPSAPS-63104: Streams Replication Manager Service Co-Located Service password default is invalid

The Streams Replication Manager Service Basic Authentication would not work with the default, random generated password. Streams Replication Manager Service Basic Authentication default password is identical on all Streams Replication Manager Service role instances without any extra actions.

Cloudera Bug: OPSAPS-63138: HBase first time setup is green although remote command failed

When Cloudera Manager does HBase replication first time setup between the given source and destination and the HBASE_REPLICATION_AUXILIARY_INFO parameter was unintentionally left there from an older HBase replication first time setup, then the 'Admin setup remote command' step failed and was ignored on the source. Therefore the HBase replication first time setup command was still displayed as successful on the destination. This has been fixed

Cloudera Bug: OPSAPS-63158: Cruise Control may not able to start after upgrade, when the initial cluster version is 7.2.14 or lower and the post-upgrade version is 7.2.14.

This issue occured when any of Cruise Control's goals lists (default-, supported-, hard-, self-healing-, anomaly detection goals) contain com.linkedin.kafka.cruisecontrol.analyzer.goals.RackAwareGoal.

Cruise Control now automatically overrides all of the deprecated RackAwareGoal occurrences with RackAwareDistributionGoal, in its configurations during a parcel upgrade.

Cloudera Bug: 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.

Cloudera Bug: 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.

Known Issues in Cloudera Manager 7.6.5

Known issues in Cloudera Manager 7.6.5

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

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

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

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

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

Cloudera bug: OPSAPS-63744: Restart of ECS needed after upgrade to Cloudera Manager 7.6.5.

If you have ECS deployed in your clusters, after upgrading Cloudera Manager to version 7.6.5, do the following in the Cloudera Manager Admin Console:

1. Restart the ECS Cluster. Go to the ECS cluster, click the actions menu and select Restart.
2. Unseal the Vault. Go to the ECS service and click ActionsUnseal .

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

Bad Message 431 reason: Request Header Fields Too Large

Workaround: Modify the Cloudera Manager Server configuration /etc/default/cloudera-scm-server file to increase the header size from 8 KB, which is the default value, to 65 KB in the Java options as shown below:

```
export CMF_JAVA_OPTS="...existing options...
-Dcom.cloudera.server.cmf.WebServerImpl.HTTP_HEADER_SIZE_BYTES=
65536
-Dcom.cloudera.server.cmf.WebServerImpl.HTTPS_HEADER_SIZE_BYTE
S=65536"
```

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

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

```
Execute command Recommission and Start on service OZONE-1
Failed to execute command Recommission and Start on service OZ
ONE-1
Recommission and Start
```

```
Command Recommission and Start is not currently available for e
xecution.
```

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

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

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

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

Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.6.5

Cloudera Manager 7.6.5 Cumulative hotfix 1

Know more about the Cloudera Manager 7.6.5 cumulative hotfixes 1.

This cumulative hotfix was released on July 14, 2022.

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

Following are the list of fixes that were shipped for Cloudera Manager 7.6.5 CHF1 (version: 7.6.5-29369964)

- **OPSAPS-64207**

  Fixed an issue where CDH 5 support for Cloudera Manager 7.6.5 was removed accidentally while removing CDH 5 support for Cloudera Manager 7.7.1 and later releases.

The repositories for Cloudera Manager 7.6.5-CHF1 are listed in the following table:

Table 1: Cloudera Manager 7.6.5-CHF1

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/redhat8/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/redhat7/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/sles12/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/ubuntu2004/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/ubuntu1804/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/43facdf3/patch-5500/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.6.5 CHF1 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

Cloudera Manager 7.6.5 Cumulative hotfix 2

Know more about the Cloudera Manager 7.6.5 cumulative hotfixes 2.

This cumulative hotfix was released on August 12, 2022.

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

Following are the list of fixes that were shipped for Cloudera Manager 7.6.5 CHF2 (version: 7.6.5-30525990)

- **OPSAPS-62007**

  When Auto-TLS is enabled, the value of the trustStorePath is overridden by the auto-generated truststore (but not the corresponding passwords) for those components where the user had manually set up TLS.This behaviour is now addressed. The truststore paths of the manually enabled TLS components are kept intact.
- **OPSAPS-62685**

  The Xstream version is upgraded to 1.4.19 version to fix CVE issues.
- **OPSAPS-63605: An Event server cannot start after an upgrade due to a field type mismatch**

  Fixed an issue where Event server failed to start after a Cloudera Manager upgrade if the value of any event attribute such as content and stack trace was longer than 32766 UTF-8 bytes.
- **OPSAPS-63759**

  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-64020**

  The Spring Framework version is upgraded to 5.3.20 version to fix CVE issues.
- **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 and now it works as intended.
- **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-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.

The repositories for Cloudera Manager 7.6.5-CHF2 are listed in the following table:

Table 2: Cloudera Manager 7.6.5-CHF2

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/redhat8/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/redhat7/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/sles12/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/ubuntu2004/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/ubuntu1804/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/0ad5a2d8/patch-5526/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.6.5 CHF2 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

Cloudera Manager 7.6.5 Cumulative hotfix 3

Know more about the Cloudera Manager 7.6.5 cumulative hotfixes 3.

This cumulative hotfix was released on October 24, 2022.

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

Following are the list of fixes that were shipped for Cloudera Manager 7.6.5 CHF3 (version: 7.6.5-33320828)

- **OPSAPS-62886**

  When there are a large number of replication policies, the Cloudera Manager Replication Replication Policies page takes a long time to load. This issue is fixed.
- **OPSAPS-64287: DAS WebUI fails to open with the "Request Header Fields Too Large" error**

  This issue has been fixed by adding a new optional parameter called das_application_connector_configs to configure the header size.

- **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-64859**

  Fixed an issue where the Replication History page does not load the history of the policy.
- **OPSAPS-65040**

  Fixed an issue where impala query processing takes a long time by Cloudera Manager Service Monitor (SMON). This fix improves the performance of ImpalaFileFormatAnalysisRule.

The repositories for Cloudera Manager 7.6.5-CHF3 are listed in the following table:

Table 3: Cloudera Manager 7.6.5-CHF3

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/redhat8/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/redhat7/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/sles12/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/ubuntu2004/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/ubuntu2004/apt/cloudera-manager.list`

Repository Type	Repository Location

Ubuntu 18	Repository:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/ubuntu1804/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/a4f2c74b/patch-5563/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.6.5 CHF3 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

Cloudera Manager 7.6.5 Cumulative hotfix 4

Know more about the Cloudera Manager 7.6.5 cumulative hotfixes 4.

This cumulative hotfix was released on December 02, 2022.

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

Following are the list of fixes that were shipped for Cloudera Manager 7.6.5 CHF4 (version: 7.6.5-34812258)

- **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.

The repositories for Cloudera Manager 7.6.5-CHF4 are listed in the following table:

Table 4: Cloudera Manager 7.6.5-CHF4

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/redhat8/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/redhat7/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/redhat7/yum/cloudera-manager.repo`

Repository Type	Repository Location

SLES 12	Repository:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/sles12/yum`
	Repository File:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/ubuntu2004/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/ubuntu1804/apt`
	Repository file:
	`http://username:password@bits.cloudera.com/32285e6a/patch-5598/ubuntu1804/apt/cloudera-manager.list`

Note: In Cloudera Manager 7.6.5 CHF4 release, you cannot use your regular paywall credentials as the repository files were published under bits.cloudera.com. Cloudera recommends you contact Cloudera Support for user credentials.

Cloudera Manager 7.6.5 Cumulative hotfix 5

Know more about the Cloudera Manager 7.6.5 cumulative hotfixes 5.

This cumulative hotfix was released on January 26, 2023.

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

Following are the list of fixes that were shipped for Cloudera Manager 7.6.5 CHF5 (version: 7.6.5-37036740)

- **OPSAPS-64520**

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

The repositories for Cloudera Manager 7.6.5-CHF5 are listed in the following table:

Table 5: Cloudera Manager 7.6.5-CHF5

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/redhat8/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/redhat7/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/redhat7/yum/cloudera-manager.repo`

SLES 12	Repository:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/sles12/yum`
	Repository File:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/sles12/yum/cloudera-manager.repo`

Ubuntu 20	Repository:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/ubuntu2004/apt`
	Repository file:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/ubuntu2004/apt/cloudera-manager.list`

Ubuntu 18	Repository:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/ubuntu1804/apt`
	Repository file:
	`https://username:password@archive.cloudera.com/p/cm7/patch/7.6.5-37036740/ubuntu1804/apt/cloudera-manager.list`