Cloudera Manager 7.11.3

Release Notes

Date published: 2020-11-30
Date modified: 2024-02-23

CLOUDERA

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.11.3 Cumulative hotfix 6 Release notes for Data Services 1.5.4

Known issues, fixed issues and new features for Cloudera Manager 7.11.3 CHF6 (version: 7.11.3.9-53216725).

What's New in Cloudera Manager 7.11.3 Cumulative hotfix 6 for Data Services 1.5.4

New features and changed behavior for Cloudera Manager 7.11.3 CHF6 (version: 7.11.3.9-53216725) in Data Services 1.5.4 release.

ECS Update Ingress Controller Certificate action is now available through the API

You can now access the ECS Update Ingress Controller Certificate action through the API and the UI.

Password protection support for Ingress private key

Ingress certificate private key is now supported with password protection.

Changed or updated features

Deploy client configuration command timed-out on larger node clusters

The Deploy Client Config command is improved now. Previously, it could take long and time-out on large clusters. It is now leveraging multithreading and optimized for parallel execution. The command is now expected to complete much faster and should not cause timeouts.

Known Issues in Cloudera Manager 7.11.3 Cumulative hotfix 6 for Data Services 1.5.4

Known issues in Cloudera Manager 7.11.3 CHF6 (version: 7.11.3.9-53216725) for Data Services 1.5.4.

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-69847:Replication policies might fail if source and target use different Kerberos encryption types

Replication policies might fail if the source and target Cloudera Manager instances use different encryption types in Kerberos because of different Java versions. For example, the Java 11 and higher versions might use the *aes256-cts* encryption type, and the versions lower than Java 11 might use the *rc4-hmac* encryption type.

Ensure that both the instances use the same Java version. If it is not possible to have the same Java versions on both the instances, ensure that they use the same encryption type for Kerberos. To check the encryption type in Cloudera Manager, search for krb_enc_types on the Cloudera Manager Administration Settings 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
```

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.

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

Fixed Issues in Cloudera Manager 7.11.3 Cumulative hotfix 6 for Data Services 1.5.4

Fixed issues in Cloudera Manager 7.11.3 CHF6 (version: 7.11.3.9-53216725) for Data Services 1.5.4 release.

OPSAPS-70207: Cloudera Manager Agents sending the Impala profile data with an incorrect header

Fixed an issue where Impala query profile data was not visible in Cloudera Observability with Cloudera Manager Agents running on Python 3. This was caused by Cloudera Manager Agents sending the profile data with an incorrect Content-Type in the HTTP header. Telemetry Publisher responded to the issue with incorrect Content-Type stopping the data flow. The issue was fixed by correcting the Content-Type header. No further action is required.

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

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

OPSAPS-60832: Decommissioning process for HDFS DataNodes is not completed in Cloudera Manager

This issue has been fixed by renewing the Kerberos ticket, which addresses Kerberos expiration issues during the DataNode decommissioning process.

OPSAPS-68418: Partition missing during column statistics import operation

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

OPSAPS-70079: NPE appears during the directory creation process in the Isilon clusters because the sourceRoleForKerberos value is null

After you configure the Dell EMC Isilon clusters, you must ensure that you configure the following options on the Cloudera Manager Administration Settings page:

- Custom Kerberos Keytab Location (to be used for replication for secure clusters on this Cloudera Manager)
- Custom Kerberos Principal Name (to be used for replication for secure clusters on this Cloudera Manager)

Tip: Use the configured Custom Kerberos Principal Name value in the Run As Username field during the replication policy creation process when using Isilon storage clusters. For more information, see How to resolve replication policies that fail with the “Custom keytab configuration is required for this service” error.

Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.11.3 cumulative hotfix 6

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.11.3 cumulative hotfix 6.

Cloudera Manager 7.11.3 CHF6

- CVE-2019-14893 - Jackson Databind
- CVE-2020-9546 - Jackson Databind
- CVE-2020-10672 - Jackson Databind
- CVE-2020-10968 - Jackson Databind
- CVE-2020-10969 - Jackson Databind
- CVE-2020-11111 - Jackson Databind
- CVE-2020-11112 - Jackson Databind
- CVE-2020-11113 - Jackson Databind
- CVE-2020-11619 - Jackson Databind
- CVE-2020-11620 - Jackson Databind
- CVE-2020-14060 - Jackson Databind
- CVE-2020-14061 - Jackson Databind
- CVE-2020-14062 - Jackson Databind
- CVE-2020-14195 - Jackson Databind

- CVE-2020-35728 - Jackson Databind
- CVE-2020-25649 - Jackson Databind
- CVE-2021-29425 - Commons-io
- CVE-2021-46877 - Jackson Databind
- CVE-2020-13697 - Nanohttpd
- CVE-2022-21230 - Nanohttpd
- CVE-2024-22243 - Spring Framework

Cloudera Manager 7.11.3 Cumulative hotfix 4 Release notes for Data Services 1.5.3

Known issues, fixed issues and new features for Cloudera Manager 7.11.3 CHF4 (version: 7.11.3.6-50817646).

What's New in Cloudera Manager 7.11.3 Cumulative hotfix 4 for Data Services 1.5.3

New features and changed behavior for Cloudera Manager 7.11.3 CHF4 (version: 7.11.3.6-50817646) in Data Services 1.5.3 release.

FIPS support for JDK11 in Zeppelin

Added FIPS support for JDK11 in Zeppelin.

Known Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 for Data Services 1.5.3

Known issues in Cloudera Manager 7.11.3 CHF4 (version: 7.11.3.6-50817646) for Data Services 1.5.3.

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-openj
dk
```

Azul Open JDK 11

For DEBs only

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

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.

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

Fixed Issues in Cloudera Manager 7.11.3 Cumulative hotfix 4 for Data Services 1.5.3

Fixed issues in Cloudera Manager 7.11.3 CHF4 (version: 7.11.3.6-50817646) for Data Services 1.5.3 release.

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-69711: Cloudera Manager - ECS Server host on RHEL 9.1 keeps getting entropy alerts

The host level entropy health test turns into BAD state if the OS version is among RHEL, Cent OS. OEL 9.x. That can cause BAD health state for the services deployed into these hosts. This issue is fixed now.

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 znode

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

Cloudera Manager 7.11.3 Cumulative hotfix 1 Release notes for Data Services 1.5.2

Known issues, fixed issues and new features for Cloudera Manager 7.11.3 CHF1.

What's New in Cloudera Manager 7.11.3 Cumulative hotfix 1 for Data Services 1.5.2

There are no New features and changed behavior for Cloudera Manager 7.11.3 CHF1 in Data Services 1.5.2 release.

Known Issues in Cloudera Manager 7.11.3 Cumulative hotfix 1 for Data Services 1.5.2

Known issues in Cloudera Manager 7.11.3 CHF1 for Data Services 1.5.2.

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-openj
dk
```

Azul Open JDK 11

For DEBs only

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

OPSAPS-68558: Cloudera Manager upgrade fails with the following error:There are 1 active commands of type GetClientConfigFiles

After upgrading from Cloudera Manager 7.9.5 to 7.11.3.2 version, the Cloudera Manager server does not start. Cloudera Manager server log displays an error about **active commands**. This scenario might occur when the Private Cloud Data Service Control Plane is actively issuing requests to Cloudera Manager while performing an upgrade.

Before Cloudera Manager upgrade make sure there are no **active commands** such as `getClientConfig`. If there are any **active commands**, then allow them to complete before kicking off the Cloudera Manager upgrade process.

Post upgrade, inspect the Cloudera Manager server log for the following error message: There are 1 active commands of type GetClientConfigFiles. This error might block Cloudera Manager to restart after the upgrade process. If Cloudera Manager restart fails due to the presence of active `getClientConfig` command, then to resolve this issue, perform the following steps:

1. Login to Cloudera Manager database.
2. Search for any active `GetClientConfigFiles` command in COMMANDS table.

```
SELECT NAME, ACTIVE  , COMMAND_ID FROM COMMANDS WHERE ACTIVE
 <> 0 AND NAME='GetClientConfigFiles';
```

3. Update the entry for the command_id found in step 2.

```
UPDATE COMMANDS SET active=0,success=false,state='CANCELLED'
 where command_id=<command_id>;
```

4. Restart the Cloudera Manager server by running the following command:

```
sudo systemctl restart cloudera-scm-server
```

OPSX-2713: ECS Installation: Failed to perform First Run of services.

If an issue is encountered during the Install Control Plane step of Containerized Cluster First Run, installation will be re-attempted infinitely rather than the command failing.

Since the control plane is installed and uninstalled in a continuous cycle, it is often possible to address the cause of the failure while the command is still running, at which point the next attempted installation should succeed. If this is not successful, abort the First Run command, delete the Containerized Cluster, address the cause of the failure, and retry from the beginning of the Add Cluster wizard. Any nodes that are re-used must be cleaned before re-attempting installation.

OPSX-735: Kerberos service should handle Cloudera Manager downtime

The Cloudera Manager Server in the base cluster must be running in order to generate Kerberos principals for Private Cloud. If there is downtime, you may observe Kerberos-related errors.

Resolve downtime on Cloudera Manager. If you encounter Kerberos errors, you can retry the operation (such as retrying creation of the Virtual Warehouse).

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

The metric definitions for kafka_connect_connector_task_metrics_batch_size_avg and kafka_connect_connector_task_metrics_batch_size_max in recent Kafka CSDs conflict with previous definitions in other CSDs. This prevents CM from registering these metrics. It also results in SMM returning an error. The metrics also cannot be monitored in CM chart builder or queried using the CM API.

Contact Cloudera support for a workaround.

Fixed Issues in Cloudera Manager 7.11.3 Cumulative hotfix 1 for Data Services 1.5.2

There are no Fixed issues in Cloudera Manager 7.11.3 CHF1 in Data Services 1.5.2 release.