CDP Private Cloud Base 7.1.4

Release Notes

Date published: 2020-07-10
Date modified: 2020-10-13

https://docs.cloudera.com/

Legal Notice

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

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

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

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

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

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

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

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

Contents

Cloudera Manager 7.1.4 Release Notes

Known Issues, Fixed Issues and New features for Cloudera Manager and CDP Private Cloud Base.

What's New in Cloudera Manager 7.1.4

New features and changed behavior for Cloudera Manager.

SLES 12 SP5 Support

SLES 12 SP5 is now supported for use with CDP Private Cloud Base 7.1.4 and higher.

New Supported Databases

The following databases are now supported for use with CDP Private Cloud Base 7.1.4 and higher:

- PostgreSQL 11.x
- Oracle 12.2.0.1 is now supported for upgrades from HDP 2.6 to CDP Private Cloud Base
- Oracle 12.2.0.3 (Not supported for upgrades from HDP 2.6 to CDP Private Cloud Base.)

Support for IBM PowerPC

IBM PowerPC is now supported for CDP Private Cloud Base with RHEL versions 7.6 and 7.7.

The following components are not supported when running on IBM PowerPC:

- Impala
- Kudu
- Ozone
- Navigator Encrypt

The supported JDK for IBM PowerPC deployments is OpenJDK 8u161 or higher.

Note: This version of OpenJDK is not available from the Cloudera download site.

Ranger Resource Mapping Server (RMS)

(Technical Preview – not for production use)

Ranger RMS enables automatic translation of access policies from Hive to HDFS.

Legacy CDH users used Hive policies in Apache Sentry that automatically linked Hive permissions with HDFS ACLs. This was especially convenient for external table data used by Spark or Hive. Previously, Ranger only supported managing Hive and HDFS policies separately. Ranger RMS allows Hive permissions to be considered during HDFS access evaluation. See Installing Ranger RMS (Technical Preview).

Fixed issues in Cloudera Manager 7.1.4

Cloudera Bug: OPSAPS-57495: The system user and group for Ranger changed from service-wide to role-specific.

Ranger role level principal for Ranger Admin, Ranger Usersync and Ranger Tagsync can now be customised from Cloudera Manager UI. In addition to this configuring of System user and System groups changed from Service-level to role-specific for components in Ranger.

Cloudera Bug: OPSAPS-57674: Knox to replace the resourceManager property in Oozie using a new service instead of using JobTrackerServiceModelGenerator in Cloudera Manager.

Cloudera Manager by default enables the new Resource Manager API service in the cdp-proxy-api topology in Knox which is used for replacing the "resourceManager" property with the actual resource manager rpc:// address when an Oozie Job is submitted.

Cloudera Bug: OPSAPS-57814: Cloudera Manager populates the newly introduced ZooKeeper SSL fields for Oozie when AutoTLS is enabled on the Cluster and SSL is enabled for ZooKeeper.

Cloudera Bug: OPSAPS-57429: Zookeeper SSL or TLS support for Oozie.

When SSL is enabled in Zookeeper, Oozie tries to connect to Zookeeper using SSL instead of a non-secure connection.

Cloudera Bug: OPSAPS-57610: Schema Registry fails to appear on Ubuntu18 configurations.

When setting up the service, the install script fails to set the "hdfs.kerberos.principal:" property. This issue is now resolved.

Cloudera Bug: OPSAPS-55940: Configuring JDBC connector jar location for Schema Registry and Streams Messaging Manager.

Now the configuration to use connector jars are provided in the default path according to the configured db type.

Cloudera Bug: OPSAPS-56457: When you set up the service, the install script fails to properly set the fs.defaultFS property.

For example, in the core-site.xml file, the fs.defaultFS property has the value abfs://bsari-azl@msisan.dfs.core.windows.net/bsari-srtest-az</value. However, in the registry.yaml file, the fsURL is abfs://bsari-azl.dfs.core.windows.net/bsari-srtest-az. @ is missing This issue is now resolved.

Cloudera Bug: OPSAPS-54386: Upgrade Swagger UI due to CVE.

In the Swagger version 42 based Cloudera Manager API client, some fields of API model objects have changed compared to the previous versions. In the Python client, several fields are migrated from type float to type integer, and in the Java client several fields are migrated from type BigDecimal to type Integer.

Cloudera Bug: OPSAPS-58007: Configuring JDBC connector jar location for Schema Registry and Streams Messaging Manager.

SchemaRegistry and Streams Messaging Manager can now use the database driver jars that are deployed to shared location (typically: usr/share/java/). Now you need not manually copy the database driver libraries to the lib folders of Streams Messaging Manager and Schema Registry.

Cloudera Bug: OPSAPS-57907:Kafka metric collector adapter causes high CPU load.

This issue is now resolved.

Cloudera Bug: OPSAPS-57467: Hardcoded parcel directory causes failure when non-standard path is used and TLS is enabled.

Eliminated hardcoded parcel directory path from the Schema Registry CSD. This issue is now resolved.

Cloudera Bug: OPSAPS-57468: Hardcoded parcel directory causes failure when non-standard path is used and TLS is enabled.

Eliminated hardcoded parcel directory path from the Streams Messaging Manager CSD. This issue is now resolved.

Cloudera Bug: OPSAPS-57539: The Streams Messaging Manager UI process does not restart.

The Streams Messaging Manager UI stop script can now kill the child processes and restart.

Cloudera Bug: OPSAPS-57745: The Streams Messaging Manager UI Server fails to start. However, status in Cloudera Manager still displays green.

Cloudera Manager now correctly displays the role status when the Streams Messaging Manager UI process fails or stops.

Cloudera Bug: OPSAPS-57867: Cloudera Manager Safety Valve evaluator does not comment out the over-ridden entry.

Safety Valve for property files will now override the existing values. This is expected to cause staleness and requires a restart.

Cloudera Bug: OPSAPS-57544: Hue is currently depending on HDFS rather than using the generic DFS connector.

Hue's HDFS dependency is now on DFS rather than HDFS. This issue is now resolved.

Cloudera Bug: OPSAPS-57113: ssl.principal.mapping.rules property configured in Cloudera Manager UI is not correctly propagated to kafka brokers.

Kafka SSL safety valve now propagates configuration containing dollar signs correctly. This issue is now resolved.

Cloudera Bug: OPSAPS-58052: Unexpected keyword argument 'exclude_versions'.

This was a typo in an annotation. This issue is now resolved.

Cloudera Bug: OPSAPS-57102: Diag bundle improvement: Increase number of Archivers and their respective timeouts.

Cloudera Manager will now be able to anticipate the number of archivers and their respective timeouts based on the size of the cluster it manages. The archivers are used while diag. bundle collection occurs. This fix will also provide user to configure the archiver count and heuristically determined scaling factor to set a timeout.

Cloudera Bug: OPSAPS-57607: redaction.py must to be sanitised for unicode characters in both regex and content.

Cloudera Manager Agent upon failing to redact with the error "UnicodeDecodeError: 'ascii' codec can't decode byte 0xc3 in position 36". This issue is now resolved.

Cloudera Bug: OPSAPS-42195: API to evict old audit table entries on demand.

Cloudera Manager Audit records can now be periodically set for truncation. An admin user can now schedule this command to run, set a batch size of old records to be truncated and configure Cloudera Manager to only keep audit records by number of days.

Cloudera Bug: OPSAPS-57934: SPNEGO fails to authenticate with external authentication.

Cloudera Manager has fixed external authentication for the API users using SPNEGO kerberos protocol, which used to fail with the error HTTP/1.1 403 Access is denied. This issue is now resolved.

Cloudera Bug: OPSAPS-57587: Cluster Template must bar export and import of variables with null values.

In Cloudera Manager, the cluster template contains key & value pairs of variables. However, for keys without any values, get exported into the cluster template's json file. This can happen even if the Cloudera Manager UI exposes the issue by showing up configuration warnings. Importing such templates to new clusters also introduces these warnings. Therefore, an export of such templates require you to replace the null value. Importing the template with such key will fail with the appropriate error message. This issue is now resolved.

Cloudera Bug: OPSAPS-57033: ParamSpec for HDFS FS_CHECKPOINT_DIR_LIST causes "Too few entries. The minimum is 1." issue.

In Cloudera Manager for HDFS's Secondary Namenode role, the parameter FS_CHECKPOINT_DIR cannot be set to null if the role is in use. However, if the role is removed from the service, for example, if HDFS HA mode is enabled, then Secondary Namenode is removed automatically. This parameter can now be set to null. This issue is now resolved.

Cloudera Bug: OPSAPS-57419: Disable the Cloudera Manager session persistence.

Cloudera Manager's session persistence is disabled by default. This issue is now resolved.

Cloudera Bug: OPSAPS-57799: Handle LDAP's user search DN with multiple spaces.

Cloudera Manager failed to parse LDAP DN and OU that contain spaces. This issue is now resolved.

Cloudera Bug: OPSAPS-54397: Upgrade Supervisor due to CVE.

Supervisor upgraded to version 3.4.0. This update remove security vulnerability CVE-2017-11610.

Cloudera Bug: OPSAPS-58059: Solr log rotation: count the number of retained log files globally instead of daily.

The count of Solr log files to retain during log rotation is counted for each day instead of all Solr logs for a particular server. This issue is now resolved.

Cloudera Bug: OPSAPS-57422: HBase 2.0 JMX GET metrics changed.

Metrics removed in HBase2 are no longer polled by Cloudera Manager. This issue is now resolved.

Cloudera Bug: OPSAPS-57410: Add Security related headers to the Streams Messaging Manager Rest API Server responses.

Strict-Transport-Security and Cache-Control are added. This issue is now resolved.

Cloudera Bug: OPSAPS-57409: Add security related header controls to all Schema Registry responses..

Added the following HTTP headers to ScemaRegistry HTTP responses: Content-Security-Policy, XSS-Protection, X-Frame options, Content-Type-Options, and Cache-control. This issue is now resolved.

Cloudera Bug: OPSAPS-56714: Misinterpretation of Impala query endTime.

Impala queries are open after they are completed. For example, in Hue they now appear on the Impala query monitoring page of Cloudera Manager upon closure, without being logged as "outside acceptance window". This issue is now resolved.

Cloudera Bug: OPSAPS-58215: Same nameservice HA schedule create query is too long for Cloudera Manager.

Using cmSource/cmTarget prefixes because of which Cloudera Manager was not processing on the 50 odd properties and passing them as is to Hive repl queries as it was too big. With the prefixes changed to cldrSource and cldrTarget, the repl queries are shorter and Hive schedule create succeeded. This issue is now resolved.

Cloudera Bug: OPSAPS-57913: When HDFS HA is enabled, Cloudera Manager now passes the HDFS name service instead of one of the active NN address to the decommission monitor.

MDecommission monitor loop in the script is now improved to retry when stdout from dfsadmin -report command is empty, which helps avoid cases where NN is too busy to report success while decommissioning might still be in progress. This issue is now resolved.

Cloudera Bug: OPSAPS-43909: Execution filter is not applied to Delete Policy.

Execution filter is now applied to Delete Policy also. This issue is now resolved.

Known Issues in Cloudera Manager 7.1.4

OOZIE-3549 Oozie fails to start when Cloudera Manager 7.x is used with Cloudera Runtime 6.x and Java 11 because Oozie does not set the trust-store password.

The issue is fixed in OOZIE-3549 and is already included in CDP 7.x but not in CDH 6.x. If you are on CDH 6.x and want to upgrade to Java 11 or your Cloudera Manager to 7.x then you must request a patch.

OPSAPS-58277 Cloudera Manager Upgrade Fails on Ubuntu 18

On Ubuntu 18 only, if CDH daemon process are running, upgrading Cloudera Manager from version 7.1.4 or below, or from version 6.3.4 or below, will fail with a Segmentation fault. You must stop all clusters before upgrading Cloudera Manager 7.1.x .

OPSAPS- 58269 Staleness in Private Cloud Base 7.1.1 cluster [Ranger, Atlas, Kudu, Spark, Livy, and Hive on Tez] after upgrading Cloudera Manager

When you upgrade Cloudera Manager from 7.1.1 or 7.1.2 to 7.1.4, a staleness for Ranger service configurations is expected due to improvement in Cloudera Manager to capture the required values for Kafka brokers, Kafka security protocol configuration, and Logging Threshold for Atlas in addition to improvements for Atlas Gateway role deployment.

You must implement the improvements and restart Ranger by taking sufficient downtime for services.

CDPQE-238 Trial installer fails when using SLES 12 SP 5

Using the cloudera-manager-installer.bin (Trial installer) to install Cloudera Manager will fail when using the SLES 12 SP5 operating system.

CDPD-17603 Java version requirements for IBM PPC

You must use OpenJDK version 8u161 or higher This version is not available from the Cloudera download site.

TSB-431: Cloudera Manager 6.x issue with the service role Resume

If a selected service role on a node is restarted and fails, and the customer clicks the "Resume" button in Cloudera Manager, the service role on all of the nodes will be restarted concurrently.

Workaround:

- Instead of performing a restart we recommend performing a stop/start of the services.
- The issue is addressed in Cloudera Manager 7.2.1 and higher versions

For more information about this issue, see the corresponding Knowledge article:Cloudera Customer Advisory: Cloudera Manager 6.x issue with service role Resume

OPSAPS-54299 – Installing Hive on Tez and HMS in the incorrect order causes HiveServer failure

You need to install Hive on Tez and HMS in the correct order; otherwise, HiveServer fails. You need to install additional HiveServer roles to Hive on Tez, not the Hive service; otherwise, HiveServer fails. See Installing Hive on Tez for the correct procedures.

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"
```

Technical Service Bulletins

TSB 2021-488: Cloudera Manager is vulnerable to Cross-Site-Scripting attack

Cloudera Manager may be vulnerable to Cross-Site-Scripting vulnerabilities identified by CVE-2021-29243 and CVE-2021-32482. A remote attacker can exploit this vulnerability and execute malicious code in the affected application.

CVE

- CVE-2021-29243
- CVE-2021-32482

Impact

This is an XSS issue. An administrator could be tricked to click on a link that may expose certain information such as session cookies.

Action required

- **Upgrade (recommended)**

  Upgrade to a version containing the fix.
- **Workaround**

  None

Knowledge article

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

TSB 2021-488: Cloudera Manager vulnerable to Cross-Site-Scripting attack (CVE-2021-29243 and CVE-2021-32482)

TSB 2021-530: Local File Inclusion (LFI) Vulnerability in Navigator

After successful user authentication to the Navigator Metadata Server and enabling dev mode of Navigator Metadata Server, local file inclusion can be performed through the Navigator's embedded Solr web UI. All files can be accessed for reading which can be opened as cloudera-scm OS user. This is related to Apache Solr CVE-2020-13941.

Impact

- Attackers can read files on the Navigator Metadata Server host with the OS user privileges running the Navigator Metadata Server.
- How to confirm the vulnerability
  - Open https://<navigator_host>:<navigator_port>/debug

    Please check for Dev-mode status. To make the exploit work, dev-mode must be enabled. Please note that restarting the NMS automatically disables dev-mode.

Action required

- **Upgrade (recommended)**

- Upgrade to Cloudera Manager 7.4.4 or higher
- Please contact Cloudera Support for patched version of Cloudera Manager 6.3.4
- **Workaround**

- For Cloudera Manager 6.x:
  - Login to the Navigator Metadata Server host and edit these files:

    ```
    /opt/cloudera/cm/cloudera-navigator-server/search-schema/sol
    r/2900/nav_elements/conf/solrconfig.xml
    /opt/cloudera/cm/cloudera-navigator-server/search-schema/sol
    r/2900/nav_relations/conf/solrconfig.xml
    ```
  - Remove the entry:

    ```
    <requestHandler name="/replication" class="solr.ReplicationH
    andler" startup="lazy" />
    ```
- For Cloudera Manager 5.x:
  - Login to the Navigator Metadata Server host and edit these files:

    ```
    /usr/share/cmf/cloudera-navigator-server/search-schema/solr/
    2900/nav_elements/conf/solrconfig.xml
    /usr/share/cmf/cloudera-navigator-server/search-schema/sol
    r/2900/nav_relations/conf/solrconfig.xml
    ```

  - Remove the entry:

    ```
    <requestHandler name="/replication" class="solr.ReplicationH
    andler" startup="lazy" />
    ```

- Restart Navigator Metadata Server
- This is a temporary solution and has to be followed-up with the recommended long term solution below.

Knowledge article

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

TSB 2021-530: CVE-2021-30131 - Local File Inclusion (LFI) Vulnerability in Navigator