

Cloudera Manager 7.3.1

## Release Notes

Date published: 2020-11-30

Date modified: 2021-03-03

# 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

**Cloudera Manager 7.3.1 Release Notes.....4**

    What's New in Cloudera Manager 7.3.1.....4

    Fixed Issues in Cloudera Manager 7.3.1..... 6

    Known Issues in Cloudera Manager 7.3.1.....8

# Cloudera Manager 7.3.1 Release Notes

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

## What's New in Cloudera Manager 7.3.1

New features and changed behavior for Cloudera Manager 7.3.1.

### **New Ranger Configuration Option for Audit Log Archival**

You can now use Cloudera Manager to configure the following:

Enable or disable Ranger Audit Log Archival (Ranger Plugin DFS Audit Enabled)

### **OPSAPS-53564: New default for auth\_to-local rules**

Default auth\_to\_local rule maps the first component of the principal name to the lowercase system user name. In case no rules are specified hadoop defaults to using DEFAULT.

### **OPSAPS-55088: The reported hostname for the Cloudera Manager agent can now be configured using the Cloudera Manager API.**

When installing an agent via the Cloudera Manager API, the agent's reported hostname can now be specified with the agentReportedHostname property.

### **OPSAPS-55800: Cruise Control should infer Kerberos and SSL settings**

The security.protocol property of CruiseControl has been removed, and now inferred from the Kafka broker configuration; affects CM  $\geq 7.2.1$  and CDH  $\geq 7.2.1$ , CM  $\geq 7.3.0$  and CDH  $\geq 7.1.6$

### **OPSAPS-57492: Custom kerberos principal support for Cruise Control**

Custom kerberos principal is configurable for Cruise Control

### **OPSAPS-57496: Custom kerberos principal support for Schema Registry**

Custom kerberos principal is configurable for Schema Registry

### **OPSAPS-57497: Custom kerberos principal support for Streams Messaging Manager**

Custom kerberos principal is configurable for SMM

### **OPSAPS-57621: New option for text-based metrics in Custom Service Descriptors (CSD)**

CSD-based services can now define and collect metrics based on enumerated text values.

See the [Cloudera Manager Extensions](#) documentation.

### **OPSAPS-57697: SMM Should Auto-Configure SRM In Cloudera Manager**

SMM auto-configures its SRM connection based on a service dependency, manual configuration options are removed; affects CM  $> 7.2.3$  with CDH  $\geq 7.2.3$ , CM  $\geq 7.3.0$  and CDH  $\geq 7.1.6$

### **OPSAPS-57949: Omid (for HBase/Phoenix) is now configurable using Cloudera Manager**

There is a new CSD-based service for Omid and there is a new HBase configuration file for Omid clients.

### **OPSAPS-57963: Expose new configuration properties for Streams Replication Manager metrics processing**

New configuration properties have been added to Cloudera Manager to support tuning the metrics processing behavior of Streams Replication Manager: secondary->primary.metrics.period, metric.grace, and metric.retention.

### **OPSAPS-58153: Schema Registry role log is not visible through the Cloudera Manager UI**

In versions before Cloudera Manager 7.2.3, Schema Registry logs are not displayed in the Cloudera Manager UI.

**OPSAPS-58397: Make the Schema Registry hashing algorithm configurable**

Added new option to Schema Registry configuration where you can change the hashing algorithm used to generate schema fingerprints. The default value is MD5.

**OPSAPS-58498: [SCM] Lower the frequency of Global Audit Commands in Cloudera Manager**

Cloudera Manager's Audit Evictor command will now run once every 23 hours.

**OPSAPS-58546: Rollback documentation is now available for upgrades from CDH 5 to CDP Private Cloud Base 7**

**Note:** If your CDH5 upgrade to CDP has failed you must rollback to CDH5 before finalizing your upgrade.

See [Rolling Back a CDH 5 to CDP 7 Upgrade](#). Read all directions before attempting a rollback.

**OPSAPS-58598: Exporting cluster configuration alters the solr-infra instance name**

New behavior for Cloudera Manager 7.3.0 and later: When imported a cluster template, each service's name will be filled in with the refname defined in the template. Previous behavior was that the service name would be the service\_type + a random number. The new behavior takes effect as long as there is no pre-existing service in Cloudera Manager with the same name. This applies to all services in Cloudera Manager across all clusters. If there is a pre-existing service with the same name, then the previous behavior takes effect, and the new service name will be the service\_type + a random number.

**OPSAPS-57097 Kerberos referrals are now disabled by default**

Previously, if kerberos was enabled and hosts were running JDK 1.8u232 or JDK 11, startup of most services failed with impersonation errors. Kerberos referrals are now disabled by default for all Java services.

**OPSAPS-58621: Custom kerberos principal support for SRM**

Custom kerberos principal is configurable for SRM

**OPSAPS-59067: Collect additional Kafka Consumer Metrics via HTTP endpoint**

New metrics about Kafka consumers are now available in the SMM service, and are now collected by Cloudera Manager from Kafka's HTTP metrics endpoint rather than being pushed from SMM into Cloudera Manager. Upon upgrade, staleness will be observed for the Kafka service's service-metrics.properties file. This is due to changes of internal representation of consumer metrics entity and will not affect changes to any existing functionality.

**OPSAPS-59119: he supported TLS protocol versions be defaulted to Hello and v1.2 for Oozie**

The default supported TLS versions for Oozie will become SSLv2Hello,TLSv1.2 instead of TLSv1,SSLv2Hello,TLSv1.1,TLSv1.2. This configuration can be changed in Cloudera Manager if you would like to use to the old behavior.

**OPSAPS-59190: SAML signature algorithm is now selectable**

You can now select a SAML signature algorithm that a SAML message is signed with. The supported algorithms are RSA-SHA1, RSA-SHA256, RSA-SHA384, and RSA-SHA512.

**Third-party software updates****OPSAPS-47379: Spring Framework Upgrade**

The Spring Framework used by Cloudera Manager has been upgraded to version 4.3.19.RELEASE.

**OPSAPS-53309: com.ning:async-http-client upgraded to version 2.12.1.**

AsyncHttpClient used by Cloudera Manager has been upgraded from version 1.9.40 to version 2.12.1.

**OPSAPS-54389: Upgrade Jython to 2.7.2**

the Jython library has been upgraded to 2.7.2.

**OPSAPS-56311: Lucene upgrade**

The Lucene version has been upgraded to 8.4.1. Due to the Lucene API changes the following parameters for Reports Manager are no longer available: Maximum Index Writer Threads, Index Writer Thread Pool Queue Size, LUCENE\_ENABLE\_OPTIMIZE (Safety Valve).

**OPSAPS-56938: Spring Data Commons for Security**

Spring Data Commons has been upgraded to 1.13.11.

**OPSAPS-59284: Upgrade org.apache.commons:commons-compress:1.18 due to CVE**

The Apache commons-compress library has been upgraded to 1.19.

## Fixed Issues in Cloudera Manager 7.3.1

Fixed issues in Cloudera Manager 7.3.1.

**Cloudera Bug: OPSAPS-48440: Misleading SOLR monitoring warnings in the agent log**

Eliminated the misleading SOLR monitoring-related warnings from the agent log file.

**Cloudera Bug: OPSAPS-49837 Test Database Connection feature of ‘add service’ wizard now supports more MySQL variants**

When adding a service, the Test Database Connection command now works when MySQL replication is enabled. This does not guarantee that the CDP service itself will work with MySQL replication using GTID, only that the DDL commands used to test the connection work with MySQL with GTID replication.

Note that cnn itself does not work with MySQL replication using GTID.

**Cloudera Bug: OPSAPS-55872: New configuration properties in the Cruise Control service**

The following properties were added to Cruise Control: self.healing.goals, hard.goals and anomaly.detection.goals.

**Cloudera Bug: OPSAPS-56239: TEZ\_JARS classpath directory configuration should not be hardcoded in hive.sh**

The parcel root directory had initially been hardcoded in various locations, causing issues if a different path was utilized. The parcels root directory is no longer hardcoded, and is now dynamically set.

**Cloudera Bug: OPSAPS-56328: Changing Kafka Connect port numbers to non-ephemeral ports**

Kafka Connect default ports are now non-ephemeral ports.

**Cloudera Bug: OPSAPS-56999: ranger.usersync.keystore.password is not overridden via safety valves**

Fixed a bug where the ranger.usersync.keystore.password configuration property specified in an Advanced Configuration Snippet did not update the password.

**Cloudera Bug: OPSAPS-57097: Disable Kerberos referrals by default for all roles**

Fixed an issue that occurred when kerberos was enabled and hosts were running JDK 1.8u232 or later, JDK 11 or JDK 13. Startup of most services failed with impersonation errors. This resolves that issue by disabling kerberos referrals by default for all Java services.

**Cloudera Bug: OPSAPS-57595: Unused Reports Manager tuning parameters have been removed**

Parameters related to older Lucene versions have been removed.

**Cloudera Bug: OPSAPS-57937: No alerts are generated when the Hbase process is in a hung state**

HBase master monitoring (canary) showed green status even if the master did not initialize yet. Added an extra check to query HBase to see whether it is up and running.

**Cloudera Bug: OPSAPS-58157: Schema Registry swagger page does not work due to CSP violation**

The Swagger interface (API Explorer) for Schema Registry now correctly renders and the browser does not report a Content Security Policy violation error.

**Cloudera Bug: OPSAPS-58617: cdp-proxy Knox topology is missing identity-assertion**

Added identity-assertion provider into the cdp-proxy Knox topology.

**Cloudera Bug: OPSAPS-58659: Create a new checkbox in Oozie configuration to control the Callback URL Kerberos enablement**

A new configuration property “Oozie Callback Servlet Authentication” has been added to the Oozie service, requiring only Kerberos-authenticated connections to the callback servlet.

**Cloudera Bug: OPSAPS-58661: Increasing default value of ZooKeeper Session Timeout in Kafka**

The default value of the ZooKeeper Session Timeout in Kafka has been increased.

**Cloudera Bug: OPSAPS-58700: Log directories aren't removed from Cruise Control metrics when a log directory is removed from Kafka**

Fixed an issue where Cruise Control capacity bootstrapping ignores deleted log directories.

**Cloudera Bug: OPSAPS-58708: Failed to log audit event in Ranger for Kafka in AutoTLS enabled cluster**

Ranger plugin's audit logging now works with non-secure Zookeeper connection while Kafka itself still uses TLS connection to Zookeeper.

**Cloudera Bug: OPSAPS-58805: Atlas hook principal configuration created with wrong principal when using multiple Hbase Masters**

The Atlas hook principal value for atlas-application.properties is now correct for HA enabled HBase clusters

**Cloudera Bug: OPSAPS-58819: Unable to set nullable fields to null with cluster template import**

The restriction on importing cluster templates with null values has been removed.

**Cloudera Bug: OPSAPS-58889: HttpFS Safety Valve configuration for core-site.xml incorrectly gets emitted to hdfs-site.xml**

HttpFS Safety Valve configurations for core-site.xml should now correctly be added to HttpFS core-site.xml.

**Cloudera Bug: OPSAPS-59021: FIPS mode Agent install reports SSL errors**

When installing agents with FIPS mode enabled, you may see the following error message:

```
Error creating custom SSL Context for the configured trustStore.  
Using default Trust Store location
```

even though the agent installation succeeds. This has been fixed.

**Cloudera Bug: OPSAPS-59081: Custom kerberos principal support for Knox**

Fixes an issue where a Knox kerberos principal configured in the Cloudera Manager Admin Console does not take effect. It is now possible to define arbitrary Kerberos principals for Knox

**Cloudera Bug: OPSAPS-59091: Upgrading from CDH->CDP sets --parquet-configurator-implementation to unsupported option Kite, which breaks all Sqoop commands**

Fixed a bug that occurred when upgrading to CDP 7.x. Cloudera Manager now sets the `parquetjob.conf.configurator.implementation` configuration property to "hadoop" for Sqoop, which is the only value supported

**Cloudera Bug: OPSAPS-59124: Kafka fails to start when there are multiple Ranger Admin roles running**

The Kafka control script in Cloudera Manager was extended to be able to handle the scenario when there are multiple Ranger Admin roles configured in the cluster and it can now correctly create the required policy repository in Ranger.

**Cloudera Bug: OPSAPS-59143: Failed to create new KafkaAdminClient from Spark Atlas Connector on TLS enabled clusters**

Fixed Atlas client configuration properties for Atlas gateway role for Atlas-Kafka SSL communication.

**Cloudera Bug: OPSAPS-59184: Incorrect Log4J configuration in Knox's control.sh script**

Fixed logging issues in Knox IDBroker and corrected log configuration file paths.

**Cloudera Bug: OPSAPS-59227: Streams Messaging Manager and Schema Registry configuration does not support the "#" character in the truststore and keystore password**

Streams Messaging Manager and Schema Registry now support the "#" character in truststore and keystore passwords.

**Cloudera Bug: OPSAPS-59248: Add support for disabling DFS audit in Schema Registry Ranger plugin**

The Schema Registry Ranger plugin no longer tries to send audits to HDFS when the `ranger_plugin_hdfs_audit_enabled` property is disabled in the Ranger configuration.

**Cloudera Bug: OPSAPS-59249: Add support for disabling DFS audit in Streams Messaging Manager (uses Kafka's Ranger plugin)**

Streams Messaging Manager's Ranger plugin no longer tries to send audits to HDFS when the `ranger_plugin_hdfs_audit_enabled` property is disabled in the Ranger configuration.

**Cloudera Bug: OPSAPS-59299: SOLR has issues if impersonating principal has a hyphen in its name**

Fixed a bug where the SOLR service had issues if the impersonating principal has a hyphen ("-") in its name.

**Cloudera Bug: OPSAPS-59340: Trying to add an HDFS Nameservice resulted in 500 Internal server error**

Fixed an issue where adding a Nameservice to HDFS via the Cloudera Manager Admin Console failed with a server error.

**Cloudera Bug: OPSAPS-59431: Console errors and performance issues on Instances page**

Improved the performance of the Select All checkbox on the Instances page for large clusters with a large number of role instances.

**Cloudera Bug: OPSAPS-59642: Hbase Replication Policy suspend action is failing (former ticket number: DMX-1405)**

Fixed an issue where suspending a Replication policy failed.

**Cloudera Bug: OPSAPS-59150: Service users created by Cloudera Manager use /bin/bash as their user shell instead of /usr/sbin/nologin.**

Service users are now created by Cloudera Manager with `/usr/sbin/nologin` and no longer use `/bin/bash` as their user shell.

## Known Issues in Cloudera Manager 7.3.1

Learn about the known issues in Cloudera Manager 7.3.1, the impact or changes to the functionality, and the workaround.

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

When using the M2Crypto 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.

**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-59511 Cloudera Manager displays invalid roles when adding role instances to the Cloudera Management Service.**

Known Issue Description: Cloudera Manager may display invalid roles when adding role instances to the Cloudera Management Service. Roles that have already been added to the Management Service may erroneously be displayed, but should not be selected.

Workaround: Ignore the extra services and continue to add the role instances.

**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.

**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-63992 – Rolling restart unavailable for SRM**

Initiating a rolling restart for the SRM service is not possible. Consequently, performing a rolling upgrade of the SRM service is also not possible.

None.

**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 2021-481: Lineage is not extracted with Cloudera Manager 7.2.x and 7.3.1 managing CDH6 or CDH5**

Cloudera Manager - Upgrade to Guava 28.1 to avoid CVE-2018-10237 triggered a Guava method version mismatch causing an exception in Navigator Metadata Server. As a result no new lineage and metadata is extracted with Cloudera Manager 7.2.4 and later with CDH6 and CDH5.

### Impact

Lineage and metadata are no longer updated in Cloudera Navigator after upgrading to Cloudera Manager 7.2.x or Cloudera Manager 7.3.1 when managing CDH5 or CDH6.

### Action required

Upgrade to the patched release of CM 7.3.1 available as PATCH-4822, or to an upcoming version later than 7.3.1. After upgrade, existing entities will have metadata extracted when extraction resumes and no lineage will be permanently lost.

### Knowledge article

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

[Cloudera Customer Advisory-481: Lineage is not extracted with Cloudera Manager 7.2.x and 7.3.1 managing CDH 6 or CDH 5](#)

### **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/solr/2900/nav_elements/conf/solrconfig.xml
```

```
/opt/cloudera/cm/cloudera-navigator-server/search-schema/solr/2900/nav_relations/conf/solrconfig.xml
```

- Remove the entry:

```
<requestHandler name="/replication" class="solr.ReplicationHandler" 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/solr/2900/nav_relations/conf/solrconfig.xml
```

- Remove the entry:

```
<requestHandler name="/replication" class="solr.ReplicationHandler" 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](#)