

CDP Private Cloud Base 7.1.2

## Release Notes

Date published: 2020-08-10

Date modified:

# CLOUDEXERA

<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 7.1.2 Release Notes.....4**
  - What's New in Cloudera Manager 7.1.2.....4
  - Known Issues in Cloudera Manager 7.1.2.....4
  - Fixed Issues in Cloudera Manager 7.1.2..... 6
- Release notes for previous versions of Cloudera Manager..... 7**

# Cloudera Manager 7.1.2 Release Notes

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

## What's New in Cloudera Manager 7.1.2

**Oracle 12.2 database is now supported by all back-end databases in CDP Private Cloud Base, with the exception of the DAS service, which requires PostgreSQL.**

### **LDAP server connectivity monitoring improvements**

LDAP server connectivity monitoring now falls back to authentication bind credentials if none are specified for monitoring. LDAP server connectivity monitoring bind credentials have been repositioned next to those authentication on the UI, with revised description for the bind DN. Cloudera Manager Server log gives more details about incomplete configuration for LDAP server connectivity monitoring.

### **Disable server side schema caching**

Server side caching in Schema Registry is now disabled.

### **Logging improvements related to YarnDeployServiceClientConfigsCommand**

YarnDeployServiceClientConfigsCommand-related logging messages have been improved.

### **New configurations to enable the Ranger plugin for Schema Registry are now available**

### **Update KTS CSD for Postgres 12**

Upgrades the embedded Postgres database used by KTS from 9.3 to 12.1 (when used with a KTS 7.1.1 or later parcel version)

## Known Issues in Cloudera Manager 7.1.2

### **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-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](#)

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

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](#)

## Fixed Issues in Cloudera Manager 7.1.2

This topic lists the issues that have been fixed in Cloudera Manager since the previous release of Cloudera Manager.

### Cloudera Bug: OPSAPS-56691: Improved log scanning scalability in Impala clusterstats

Fixed completed Impala query monitoring for large query profiles by improving log scanning scalability.

### Cloudera Bug: OPSAPS-54869: Spurious errors about missing mounts

Fixed spurious errors about missing mounts that were logged by the agent when user runtime directories in /run/user are removed normally.

### Cloudera Bug: OPSAPS-56607: Monitor daemon fails to remove principal

Fixed an issue where the Cloudera Manager Agent produces the following error when regenerating credentials for a service:

```
[18/Apr/2020 01:09:25 +0000] 13158 CredentialManager kt_renewer
WARNING Couldn't kinit as 'solr/lpc6001cdp02.grupocgd.com' using
/var/run/cloudera-scm-agent/process/1546364905-solr-SOLR_SERVER/solr.keytab - kinit:
Client's credentials have been revoked while getting initial credentials
```

**Cloudera Bug: OPSAPS-55540: Cloudera Manager - Compute Cluster - Schema Registry first run fails with "failed to find service class" error**

This failure has been fixed.

**Cloudera Bug: OPSAPS-56498: Spark compute cluster failing to start when Oozie start fails**

Fixed failure to start virtual private cluster for Spark.

**Cloudera Bug: OPSAPS-56153: [SCM] Diagnostic bundle uploads fail to authenticate with Proxy**

Cloudera Manager diagnostic bundle uploads have fixed the 407 authentication exception issue, when a diagnostic bundle was uploaded using a proxy server with basic authentication.

**Cloudera Bug: OPSAPS-55608: Failed to upgrade KTS KMS to Ranger KMS**

Fixed an issue where the Ranger KTS KMS service was failing to start when the configuration is present in a non-default location.

**Cloudera Bug: OPSAPS-56561: Zookeeper time out during upgrade**

In large cluster, the resetAcls command takes a longer time to complete. To prevent timeouts while the command is running, the time out value is now set to NO\_TIMEOUT.

**Cloudera Bug: OPSAPS-55038: QueueManager config error in 7.0.3 cluster after upgrade to Cloudera Manager 7.1.1.**

Fixed an issue where the Custom Service Descriptor (CSD) referenced an incorrect version of Cloudera Manager, causing a failure in QueueManager during upgrade.

**Cloudera Bug: OPSAPS-53158: "Command Succeeded but fetching results failed" caused by FD limit**

Fixes a file descriptor leak by the Cloudera Manager Agent's HTTP status server when Auto-TLS is enabled. The fix applies to all supported operating systems, except for Redhat 6-based systems.

**Cloudera Bug: OPSAPS-56468: Setting a large value to YARN Localized Dir deletion delay setting makes NodeManagers fail to start**

The allowed values for the YARN Localized Dir Deletion delay configuration parameter are now limited to the maximum value of an Integer.

**Cloudera Bug: OPSAPS-56441: Add impala setAcl commands in postupgrade step**

After upgrade to CDP7.1.1, impala doesn't have permissions for the Hive warehouse directory. This is because impala's setAcl commands were not included in the upgrade process. The commands are now included.

**Cloudera Bug: OPSAPS-56785: Atlas should use actual Kafka broker security protocol rather than calculate it**

Atlas now uses the actual Kafka Broker value instead of calculating it based on Kerberos and TLS being enabled.

## Release notes for previous versions of Cloudera Manager

### CDP Data Center

- [Cloudera Manager 7.0.3 Release Notes](#)
- [Cloudera Manager 7.1.1 Release Notes](#)

### CDP Public Cloud

- [Cloudera Manager 7.0.0 Release Notes](#)
- [Cloudera Manager 7.0.1 Release Notes](#)
- [Cloudera Manager 7.0.2 Release Notes](#)
- [Cloudera Manager 7.1.0 Release Notes](#)