

CDP Public Cloud 7.2.6

## Release Notes

Date published: 2020-11-25

Date modified: 2020-12-03

# CLOUDBERA

<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

<b>Cloudera Manager 7.2.6 Release Notes.....</b>	<b>4</b>
Fixed Issues in Cloudera Manager 7.2.6.....	4
Known Issues in Cloudera Manager 7.2.6.....	4

## Cloudera Manager 7.2.6 Release Notes

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

### Fixed Issues in Cloudera Manager 7.2.6

Fixed issues in Cloudera Manager 7.2.6

**Cloudera Bug: OPSAPS-58488: Streams Messaging Manager can now connect to Ranger without errors.**

Fixed a bug that prevented Streams Messaging Manager from communicating with Ranger.

**Cloudera Bug: OPSAPS-57907: Kafka metric collection causes high CPU load**

Fixed a bug that caused high CPU load when collecting Kafka metrics on clusters with a large number of topic partitions.

**Cloudera Bug: OPSAPS-58319 Kafka metrics deleted after cluster restart.**

Fixed a bug that caused Kafka metrics to be deleted after a cluster restart.

**Cloudera Bug: OPSAPS-58708 Kafka audits were not being collected by Ranger**

Fixed a bug where Kafka audits were not collected because of an invalid TLS connection configuration to ZooKeeper.

**Cloudera Bug: OPSAPS-58733: Unable to upload diagnostic bundles when proxy username is blank**

This change fixes the issue of Cloudera Manager being unable to upload the diagnostic bundle via proxy, if a proxy user name is not provided.

**Cloudera Bug: OPSAPS-58153 Schema Registry Role log not available in the Cloudera Manager Admin Console**

Fixed a bug that prevented the display of Schema Registry logs.

**Cloudera Bug: OPSAPS-58157 Error in the Schema Registry Swagger (API Explorer) page**

Fixed a bug that caused a Content Security Policy violation error when accessing the Schema Registry Swagger (API Explorer) page.

**Cloudera Bug: OPSAPS-58847: TLS v1.2 is now supported by Atlas.**

**Cloudera Bug: OPSAPS-58537**

Fixed a bug that occurred when restarting a Data Hub cluster. The Knox and Spark Zookeeper quorum configurations incorrectly pointed to the Zookeeper service on Data hub, if there was a Zookeeper service present in the Data Hub cluster.

### Known Issues in Cloudera Manager 7.2.6

Learn about the known issues in Cloudera Manager 7.2.6, the impact or changes to the functionality, and the workaround.

**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 2021-472: Customer Advisory for Navigator Metadata Server startup issue

If the Navigator Metadata Server is executing purge, and the clean up process is interrupted, the Navigator Metadata Server will not be able to restart.

#### Impact

Navigator Metadata Server cannot be restarted if the process is killed or crashes during executing a purge. Error message:

```
[Update NAV_EXTRACTOR_STATUS set ENABLED_FOR_NEXT_EXTRACTION
= 'true']; SQL state [72000]; error code [12899]; ORA-12899: value too large for column
"NAVMS"."NAV_EXTRACTOR_STATUS"."ENABLED_FOR_NEXT_EXTRACTION" (actual:
4, maximum: 1; nested exception is java.sql.SQLException: ORA-12899: value too large for
column
"NAVMS"."NAV_EXTRACTOR_STATUS"."ENABLED_FOR_NEXT_EXTRACTION" (actual:
4, maximum: 1)
```

#### Action required

- Upgrade:
  - Cloudera Manager 6.3.4: Request a patch (PATCH-4489).
  - Cloudera Manager 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6 and 7.3.0: Upgrade to a Cloudera Manager version containing the fix.
- Workaround:
  1. Log in to the Navigator Metadata Server database.
  2. Update `NAV_MAINTENANCE_HISTORY` set `STATUS = "INCOMPLETE"` where `STATUS` like `'IN_PROGRESS'`.
  3. Update `NAV_EXTRACTOR_STATUS` set `ENABLED_FOR_NEXT_EXTRACTION = 1` where `ENABLED_FOR_NEXT_EXTRACTION = 0`.
  4. NMS is able to start and extractors are enabled.

#### Knowledge article

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

[Cloudera Customer Advisory-472: Navigator Metadata Server startup issue](#)

### 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 2021-491: Authorization Bypass in Cloudera Manager (CVE-2021-30132/CVE-2021-32483)**

Cloudera Manager (CM) 7.4.0 and earlier versions have incorrect Access Control in place for certain endpoints. A user who has a knowledge to the direct path of a resource or a URL to call a particular function, can access it without having the proper role granted. The vulnerable endpoints were CVE-2021-30132 /cmf/alerts/config?task= and CVE-2021-32483 /cmf/views/view?viewName=.

**CVE**

- CVE-2021-30132
  - Alerts config - 4.3 (Medium)
  - [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N](#)
- CVE-2021-32483
  - Views - 4.3 (Medium)
  - [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N](#)

**Impact**

A user with read only privilege is able to see configuration information in the UI.

**Action required**

Upgrade to a version containing the fix.

**Knowledge article**

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-491: Authorization Bypass in Cloudera Manager \(CVE-2021-30132 / CVE-2021-32483\)](#)