Cloudera Manager 7.0.1

Release Notes

Date published: 2020-02-11
Date modified:

https://docs.cloudera.com/

Legal Notice

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.

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

What's New in Cloudera Manager

The following pages describe new features in each release of Cloudera Manager.

What's New in Cloudera Manager 7.0.1

This topic describes new features in Cloudera Manager.

- Auto TLS

  You can now use Cloudera Manager to Automatically configure TLS for your clusters.

What's New in Cloudera Manager 7.0.0

This topic describes new features in Cloudera Manager.

What's New for Cloudera Enterprise Customers

- Apache Ranger now provides security authorization and auditing services previously provided by Sentry.

  See:

  - Apache Ranger Auditing
  - Apache Ranger Authorization
- Apache Atlas now provides data governance capabilities previously provided by Cloudera Navigator. See: Apache Atlas
- Cloudera Manager now provides configuration and management for the following Cloudera Runtime services:

  - Hive-on-Tez
  - Hive 3
  - Zeppelin
  - Livy

Important: Because cluster creation and management is provided by the Cloudera Data Hub service, the version of Cloudera Manager included with CDP provides a subset of functionality that Cloudera Manager has provided previously. Only functionality available to the Configurator user role is available.

See Cloudera Data Hub.

What's New for Hortonworks Data Platform Customers

- Cloudera Manager now provides cluster management capabilities previously provided by Ambari.

  Cloudera Manager provides the following:

  - Monitoring and alerts
  - Configuration management
  - Host management
  - Cloudera Runtime Service management
  - Resource management
  - Upgrades

  See Cloudera Manager Overview
- Apache Impala Cloudera Manager provides configuration and management for the Apache Impala service, which provides high-performance, low-latency SQL queries on data stored in popular Apache Hadoop file formats. See Apache Impala Overview

Fixed Issues

This document describes fixed issues for Cloudera Manager <version> with Cloudera Data Platform <version>.

Fixed issues in Cloudera Manager 7.0.1

This topic describes fixed issues in this release of Cloudera Manager.

OPSAPS-50447: Fixed an issue where the Health Test for Hive Metastore Server Canary fails to perform its task of checking HMS basic functionality (creating a database, table and partitions and then dropping them) and therefore reports bad health status in all cases.

Known Issues in Cloudera Manager

This document describes known issues and workarounds for using Cloudera Manager.

Known Issues in Cloudera Manager 7.0.1

This topic describes known issues and workarounds for Cloudera Manager.

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 Bulletin

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)

Known Issues in Cloudera Manager 7.0.0

This topic describes known issues and workarounds for Cloudera Manager.

Stopping a cluster using Cloudera Manager loses connection to Cloudera Manager on next start

Workaround: Do not use Cloudera Manager to stop a cluster. Instead, stop the cluster from the Management Console Data Hub Service page.

See: Stop a Cluster

OPSAPS-50447 Health Test for Hive Metastore Server Canary fails to perform its task of checking HMS basic functionality (creating a database, table and partitions and then dropping them) and therefore reports bad health status in all cases.

Workaround: Suppress the alert in Cloudera Manager.

Fixed in: Cloudera Manager 7.0.1

OPSAPS-51786: The default value for the Scheduled Diagnostic Data Collection Time configuration property contains a very old date. However, only the time portion is used to create this configuration.

Workaround:When editing this property, enter any date (this will be ignored) and the time when you want diagnostic data collection to occur.

Technical Service Bulletin

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)