Cloudera Manager 7.1.3

Release Notes

Date published: 2020-08-10
Date modified:

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.1.3 Release Notes

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

What's New in Cloudera Manager 7.1.3

New features and changed behavior for Cloudera Manager.

New supported operating systems

The following operating systems are now supported for fresh installations or upgrade to Cloudera Manager 7.1.3 and higher and Cloudera Runtime 7.1.3 and higher:

- Ubuntu 18 (not supported with Schema Registry)
- RHEL 7.8

Changed Behavior

New Cloudera Manager API endpoint for Ozone credentials

A new endpoint has been added to create an Ozone S3 bucket with a specified name, and return Ozone AWS credentials.

The new endpoint is under ClusterResource:

```
/getOzoneS3Credentials
```

The time to reindex the fsimage has been reduced

The Report Manager fsimage indexing time has been reduced, in order to handle large fsimages in a reasonable amount of time.

A new Cloudera Manager API endpoint has been added to create a custom Hive Warehouse Directory

The new endpoint is:

```
POST /clusters/{clusterName}/services/{serviceName}/commands/hiv
eCreateHiveWarehouseExternal
```

The endpoint creates a Hive warehouse external directory with the specified name.

Fixed Issues in Cloudera Manager 7.1.3

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

Cloudera Bug: OPSAPS-57414: Ozone Ranger default policies should allow bucket creation for 'hive' user to s3v volume.

Ranger's default policy now allows Hive user access to an Ozone s3v volume.

Cloudera Bug: OPSAPS-57254: Agent reporting hangs indefinitely when there is a problem with the SSL connection.

Fixed an issue that occurred when the agent encountered a problem with the SSL connection while reporting to the HostMonitor. Reporting hung indefinitely causing the entire node to be marked as in Bad Health. Now, a problem with the SSL connection will no longer block the agent from reporting.

Cloudera Bug: OPSAPS-56870: Provide a way for non-administrators to get the truststore password

The API endpoints /api/v40/certs/truststore and /api/v40/certs/truststorePassword are now accessible by users with read-only permissions. These APIs return the truststore and truststore password that is configured with the Cloudera Manager TLS/SSL Client Trust Store File Location and Cloudera Manager TLS/SSL Client Trust Store Password configuration parameters, respectively.

Cloudera Bug: OPSAPS-56479: Different clusters using same Cloudera Manager are gathering collection metrics from all Solr services and displaying all the collections from all the clusters.

Fixed an issue where different clusters managed by the same Cloudera Manager instance and having multiple Solr services were displaying every collection for every service under the Collection tab.

Different clusters managed by the same Cloudera Manager instance and having multiple HBase services were displaying every HTable for every service under the HTable tab.

Now, collection statistics are only shown for the correct specific HBase or Solr instance.

Cloudera Bug: OPSAPS-56130: Ozone Gateway Advanced Configuration Snippets are not included in the Ozone client configuration

Ozone configuration properties specified in the Ozone Service Advanced Configuration Snippet (Safety Valve) for ozone-conf/ozone-site.xml configuration property are now included in the client configurations.

Cloudera Bug: OPSAPS-57377: Cloudera Manager allows addition of multiple Role Instances for Storage Container Manager

Fixed an issue where multiple Ozone Storage Container Manger (SCM) instances could be added using Cloudera Manager. Cloudera Manager now only allows one instance to be added per Ozone service.

Cloudera Bug: OPSAPS-57560: "Setup HDFS Data at Rest Encryption" shows as red even with RangerKMS enabled

Fixed an issue where "Setup HDFS Data at Rest Encryption" under CM -> Administration -> Security showed as red even after Ranger KMS was enabled.

Known Issues in Cloudera Manager 7.1.3

Cloudera bug OPSAPS-57524: Extra Installation step required for Ubuntu 18 with Ranger and Kudu

If you are installing Cloudera Manager on Ubuntu, and are planning to add the Kudu service to the cluster and are planning to enable Apache Ranger, run the following command on all cluster hosts before installing Cloudera Manager:

```
sudo apt-get install gettext-base
```

If you know in advance which hosts will be running the Kudu service roles, you only need to run this command on those hosts.

Cloudera bug: CDPD-15937: Ubuntu 18 Support

Schema Registry is not supported when using Ubuntu 18.

CDPD-13222: Apache Ranger Setup fails on existing cluster

If Apache Ranger was not added to the cluster during its initial creation you must use the following manual steps to add Apache Ranger:

1. Log in to the Cloudera Manager Admin Console.
2. Add a new Solr service.
3. Set the value of the Solr configuration parameter ZooKeeper ZNode to solr-infra.
4. Add the Apache Ranger service. When prompted, select the newly-created Solr service.

See Adding a Service.

Cloudera bug: 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-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"
```

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.

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