Cloudera Manager 7.2.0

Release Notes

Date published: 2020-05-28
Date modified: 2020-06-16

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.2.0 Release Notes

Known Issues, Fixed Issues and New features for Cloudera Manager and CDP Data Center.

What's New in Cloudera Manager 7.2.0

New and changed features in Cloudera Manager 7.2.0.

Cloudera Bug: OPSAPS-56578: Increase default CMCA expiration to 5 years

The default lifespan of the automatically generated internal Certificate Authority for Auto TLS has been increased from 1 year to 5 years

Cloudera Bug: OPSAPS-54988: Tag all Kerberos configurations to enable when services are added to a Kerberized cluster

When a new service is added to a cluster that is already kerberized, kerberos settings will automatically be configured for the new service.

Cloudera Bug: OPSAPS-55598: Expose hive.server2.tez.sessions.per.default.queue config for Hive in CM UI

Parameter hive.server2.tez.sessions.per.default.queue config is now exposed.

Cloudera Bug: OPSAPS-55276: Add configuration property to enable / disable YARN recommendation engine APIs

The YARN Recommendation API will recommend scaling up or down the nodes based on the demand/idle state of cluster resources. This can be turned on/off using the YARN configuration property yarn.cluster.scaling.recommendation.enable.

Cloudera Bug: OPSAPS-54643: The Guava version for Cloudera Manager 28.1 to avoid CVE-2018-10237

Guava library has been upgraded to version 28.1-jre. R

Cloudera Bug: OPSAPS-55842: Update Apache POI dependency from outdated 3.16 due to multiple CVEs

The Apache POI has been upgraded to v4.1.0.

Known Issues in Cloudera Manager 7.2.0

Learn about the known issues in Cloudera Manager 7.2.0, the impact or changes to the functionality, and the workaround.

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)

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 2022-507 Certificate expiry issue in CDP

The Transport Layer Security (TLS) keystore needs to be manually rotated due to an issue with certificate rotation.

The Root Cause Analysis is that the keystore path of the Cloudera Manager (CM) server is set to a directory based on the non-FQDN (Fully Qualified Domain Name) of the CM server. However, the certificate rotation on a directory happens based on the FQDN of the CM server. This results in a situation in which the keystore of the CM server does not get updated.

Impact

The clusters could experience downtime.

Action required

- Workaround if the certificates have not yet expired:
  1. Back up the existing host keystore from the directory based on the hostname of the CM server. Example:

     ```
     cp -R /etc/cloudera-scm-server/certs/hosts-key-store/example-datalake-1-master0/ /etc/cloudera-scm-server/certs/hosts-key-store/example-datalake-1-master0.backup
     ```

  2. Copy the keystore from a directory based on the FQDN of the CM server. Example:

     ```
     cp -Rf /etc/cloudera-scm-server/certs/hosts-key-store/example-datalake-1-master0.domain.site/* /etc/cloudera-scm-server/certs/hosts-key-store/example-datalake-1-master0/
     ```

  3. Restart the CM server
  4. Confirm that OpenSSL now shows a certificate with the expected expiration time. Example:

     ```
     openssl s_client -connect $(grep "server_host" /etc/cloudera-scm-agent/config.ini | sed s/server_host=//):7182 </dev/null | openssl x509 -text -noout
     ```

  5. Repeat these steps after each host certificate rotation.

- Workaround if the certificates have already expired:
  1. You must run commands on each host with expired certificates to regenerate new ones.
  2. For each affected host (including the Cloudera Manager server host if necessary), let “<hos t_FQDN>” be the fully-qualified domain name of that host:
     a. Run the following command on the Cloudera Manager server host as root:

```
/opt/cloudera/cm-agent/bin/certmanager --location
/etc/cloudera-scm-server/certs gen_node_cert --rotate --o
utput=/tmp/<host_FQDN>.tar <host_FQDN>
```

     b. Copy /tmp/<host_FQDN>.tar to the affected host.
     c. Run the following commands on the affected host as root:

     - ```
       /opt/cloudera/cm-agent/bin/cm install_certs /tmp/<ho
       st_FQDN>.tar
       ```
     - ```
       chmod 755 /var/lib/cloudera-scm-agent/agent-cert/
       ```

  3. Restart Cloudera Manager by running the following command on the Cloudera Manager server host as root:

```
service cloudera-scm-server restart
```

  4. Restart the Knox service by running the following commands on the Cloudera Manager server host as any user, replacing “UpdateWithYourUser” and “UpdateWithYourCluste rName” with the workload user and cluster name, respectively:

     - ```
       WORKLOAD_USER="UpdateWithYourUser"
       ```
     - ```
       CM_SERVER="http://$(hostname -f):7180"
       ```
     - ```
       CM_API_VERSION=$(curl -s -L -k -u ${WORKLOAD_USER} -X GET
                    "${CM_SERVER}/api/version") && echo ${CM_API
       _VERSION}
       ```
     - ```
       CM_CLUSTER_NAME=<UpdateWithYourCusterName>
       ```
     - ```
       KNOX_SERVICE_NAME=$(curl -s -L -k -u ${WORKLOAD_USER} -X
        GET
                    "${CM_SERVER}/api/${CM_API_VERSION}/clust
       ers/${CM_CLUSTER_NAME}/services/" | awk -F
                    "[ |:|,]" '/name.*knox/ {print $(NF - 1 )}'
        | sed 's|"||g') && echo
                    ${KNOX_SERVICE_NAME}
       ```
     - ```
       curl -s -L -k -u ${WORKLOAD_USER} -X POST
                    "${CM_SERVER}/api/${CM_API_VERSION}/clusters
       /${CM_CLUSTER_NAME}/services/${KNOX_SERVICE_NAME}/comman
       ds/restart"
       ```

  5. Follow the steps in the above section: “Workaround if the certificates have not yet expired”

Knowledge article

For the latest update on this issue, please see the corresponding Knowledge article: TSB 2022-507: Certificate expiry issue in CDP

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)

Fixed Issues in Cloudera Manager 7.2.0

Issues that have been fixed in Cloudera Manager since the previous release.

Cloudera Bug: OPSAPS-56457: Schema Registry yaml file generation broken on Azure.

The YAML file is now generated correctly.

Cloudera Bug: OPSAPS-55564: Increase the max length of configuration values in the Postgresql schema

The maximum size of a configuration value that can be persisted when running on PostgresSQL has been increased from 1 MiB to 1GiB, which more closely matches the behavior of Oracle and MySQL databases.

Cloudera Bug: OPSAPS-56269: Multiple Operational Database clusters should use different Ranger policies

Issue has been fixed.

Cloudera Bug: OPSAPS-55387: NPE during Cloudera Manager cluster template importing

Fixed a bug that caused a null pointer exception when importing cluster templates.

Cloudera Bug: OPSAPS-56286: Schema Registry Health Check broken with multiple instances

Heath test fixed for Schema Registry when there are multiple instances of Schema Registry deployed.

Cloudera Bug: OPSAPS-56345: Issues with Schema Registry's Ranger repo handling

Ranger init script was rewritten to generate the repo name with a unique name. It will also not fail in case the repo already exists.

Cloudera Bug: OPSAPS-56650: Generate Missing Credentials Fails due to issue with 'ldapdelete' command

The components in DomainNames (DNs) viz. cn, dc, ou are valid even with whitespaces due to which the generate missing credentials script in Cloudera Manager failed. This is now fixed.

Cloudera Bug: OPSAPS-56210: Upgrade failed with Oracle12 with "Failed to Create Hive Sys Database"

Fix to the COLUMN name in the Oracle schema file.

Cloudera Bug: OPSAPS-57000: Disable IDBroker token renewal

Modified IDBroker configuration so that server-management of token state is disabled (token renewal/revocation is also disabled as a result).

Cloudera Bug: OPSAPS-56442: Deploying CB template results in Error

We opened two follow-up jiras based on further testing and debugging. Hence marking this as resolved. https://jira.cloudera.com/browse/OPSAPS-56576 https://jira.cloudera.com/browse/CDPD-12612

Cloudera Bug: OPSAPS-53101: Hue cannot install sample_07 table, connection error

This issue has been fixed.

Cloudera Bug: OPSAPS-54424: yarn_kerberos_cluster installation failure: Failed to generate client configuration. (error 500)

The Deploy client configuration command can fail easily if the HostStatus of the host heartbeat that includes component version is not received for hadoop-mapreduce. This command now waits for these heartbeats,