Cloudera Manager 7.1.0

Release Notes

Date published: 2020-02-11
Date modified:

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.1.0 Release Notes

Fixed Issues in Cloudera Manager 7.1.0

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

Cloudera Bug: OPSAPS-54084: Cloudera Manager no longer logs sensitive configuration parameters when reading the init file

Fixed an issue where values of sensitive configuration parameters might be logged to the cloudera-scm-server.log when they are set using the "-i" argument to Cloudera Manager Server.

Cloudera Bug: OPSAPS-53981: Gracefully handle cyclic dependency exception during configuration validation

Fixed an issue where setting a Solr service to depend on a Ranger service that already depends on the Solr service would cause a cyclic dependency exception.

Cloudera Bug: OPSAPS-51606: Null pointer exception when a configuration value is empty

Fixes a null pointer exception that occurred when a numeric parameter is set to an empty value. Cloudera Manager will use the default value if there is one.

Cloudera Bug: OPSAPS-54100: Impala Bytes Streamed parameter missing due to profile format change

Metrics monitoring is now fixed for Impala when using KRPC "streamed bytes" .

Cloudera Bug: OPSAPS-52988: Application Diagnostic bundle collection does not work for MapReduce jobs.

Fixed an issue where MapReduce jobs were not being collected in the YARN Application Bundle.

Cloudera Bug: OPSAPS-52680: Kafka MirrorMaker fails to start if topic whitelist configuration property is not specified

Kafka MirrorMaker whitelist parameter is now required to ensure that the MirrorMaker process can start.

Cloudera Bug: OPSAPS-52115: Hive service should not depend on Spark starting with C7

Hive on Spark related parameters will not appear in the Hive service configuration.

Cloudera Bug: OPSAPS-53818: Update configuration values to reduce instability from stuck ServerCrashProcedures

The default value for the hbase.master.namespace.init.timeout configuration property has been changed to 1800000 ms.

Cloudera Bug: OPSAPS-44250: Add validation for encryption algorithm etc.

If the dfs.encrypt.data.transfer property is enabled and the dfs.encrypt.data.transfer.algorithm proprrty is not set to AES/CTR/NoPadding then a warning message is displayed that indicates poor DataNode performance.

Cloudera Bug: OPSAPS-53925: Cloudera Manager agent logs are not showing the correct timezone on the log's timestamp

The cloudera-scm-agent.log file entries now display timestamps with the correct offset based on the timezone of the host.

Known Issues in Cloudera Manager 7.1.0

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 Bulletins

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-ke
     y-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/exampl
     e-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/nul
     l | 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 (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)

What's New in Cloudera Manager 7.1.0

Cloudera Issue: OPSAPS-53169, OPSAPS-53636
The time required to create a cluster has decreased by up to 4 minutes.

Cloudera Issue: OPSAPS-51403: Support for Solr plugins has been added for workload clusters

Cloudera Issue: OPSAPS-43085: The HDFS directory usage report now allows you to select the size of the CSV download file

You can select on of the following options for downloading:

- Top 1K rows
- Top 10k rows
- Top 100k rows

Cloudera Issue: OPSAPS-46007: New configuration parameters to add the ability to specify max_retries for service auto-restart

Two new configuration fields have been added on all Roles: Start Wait Timeout and Start Retry Attempts, located in the Advanced category. These fields control how many times a role's process is automatically restarted if the process exits or crashes during startup.

Startup is defined as a duration of Start Wait Timeout in seconds.

Start Retry Attempts is the number of times the process will get restarted before giving up.

After a process has been running longer than Start Wait Timeout seconds, the restarts count is set back to zero.

Cloudera Issue: OPSAPS-28229: Support for HTTP Strict Transport Security Mode

When TLS is enabled for the Cloudera Manager Admin Console, web requests will now include the Strict-Transport-Security header. For more details on this header, see Mozilla's documentation: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Cloudera Issue: OPSAPS-52546: HBase thrift http server and proxy user are enabled if Hue and HBase are both installed

When Hue is used with HBase, the following configuration parameters are now set in HBase:

```
hbase.regionserver.thrift.http = true
hbase.thrift.support.proxyuser = true
```

Cloudera Issue: OPSAPS-54069: SPNEGO for Impala's webui is on by default with Kerberos

Impala's Web UI is now automatically protected with Kerberos whenever it is configured on a cluster.

Cloudera Issue: OPSAPS-53826: Add Granular permissions to Tags

Tags will only be accessible via the TagsResource API if the user has correct permissions. Any role with read permissions grants read access to tags, and a Configurator, Limited Cluster Administrator, Cluster Administrator, or Full Administrator role is required to add or delete tags.

Cloudera Issue: OPSAPS-53341: New property in HBase

Added the following HBase configuration properties: hbase.use.dynamic.jars and hbase.dynamic.jars.dir properties. For new installations of Cloudera Runtime 7.1 or later, the hbase.use.dynamic.jars property is set to false by default.

Cloudera Issue: OPSAPS-53957: Phoenix Query Server memory options are configurable

It is now possible to set the Heap Size for Phoenix Query server.

Cloudera Issue: OPSAPS-54062: Zookeeper SSL/TLS support for Kafka

A new Kafka configuration parameter, zookeeper.secure.connection.enable has been added to allow Kafka to connect and communicate to Zookeeper through a secure channel. This configuration only takes effect if TLS is enabled on the Zookeeper server.

Cloudera Issue: OPSAPS-30763: New Kafka configuration parameter

The Kafka configuration parameter, zookeeper.set.acl, when set to true, causes Kafka to create Zookeeper nodes as world readable and creator writable, as opposed to the default of world readable and writable. This prevents unauthorized users from changing data in Zookeeper.

Cloudera Issue: OPSAPS-53340: PAM authentication is now configurable in Kafka CSD

You can now configure PAM configuration to allow Kafka clients to authenticate using Linux-PAM.

Cloudera Issue: OPSAPS-48218

Cloudera Manager configures the hbase.thrift.spnego.principal and hbase.thrift.spnego.keytab.file properties for HBase Thrift server.

Cloudera Issue: OPSAPS-53785: New HDFS configuration parameter

A new HDFS configuration parameter "Enable Async Audit Log" has been added. It is enabled by default for Cloudera Runtime 7.1.0 and later. When enabled, HDFS NameNode will append the audit log asynchronously when using the HDFS default audit logger. Enabling this parameter can improve NameNode throughput under heavy load.

Cloudera Issue: CDPD-6477

Cloudera Manager’s Auto-TLS feature now supports Apache Kudu.