Cloudera Manager 7.3.0

Release Notes

Date published: 2020-11-30
Date modified: 2021-02-10

CLOUDERA

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.3.0 Release Notes

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

What's New in Cloudera Manager 7.3.0

New features and changed behavior for Cloudera Manager.

Cloudera Bug: OPSAPS-58397: Make the Schema Registry hashing algorithm configurable

Added new option to Schema Registry configuration where you can change the hashing algorithm used to generate schema fingerprints. The default value is MD5.

Cloudera Bug: OPSAPS-57697: SMM Should Auto-Configure SRM In Cloudera Manager

SMM auto-configures its SRM connection based on a service dependency, manual configuration options are removed; affects CM > 7.2.3 with CDH >= 7.2.3, CM >= 7.3.0 and CDH >= 7.1.6

Cloudera Bug: OPSAPS-55800: Cruise Control should infer Kerberos and SSL settings

The security.protocol property of CruiseControl has been removed, and now inferred from the Kafka broker configuration; affects CM >=7.2.1 and CDH >= 7.2.1, CM >= 7.3.0 and CDH >= 7.1.6

Cloudera Bug: OPSAPS-58498: [SCM] Lower the frequency of Global Audit Commands in Cloudera Manager

Cloudera Manager's Audit Evictor command will now run once every 23 hours.

Cloudera Bug: OPSAPS-58153: Schema Registry role log is not visible through the Cloudera Manager UI

In versions before Cloudera Manager 7.2.3, Schema Registry logs are not displayed in the Cloudera Manager UI.

Cloudera Bug: OPSAPS-58598: Exporting cluster configuration alters the solr-infra instance name

New behavior for Cloudera Manager 7.3.0 and later: When imported a cluster template, each service's name will be filled in with the refname defined in the template. Previous behavior was that the service name would be the service_type + a random number. The new behavior takes effect as long as there is no pre-existing service in Cloudera Manager with the same name. This applies to all services in Cloudera Manager across all clusters. If there is a pre-existing service with the same name, then the previous behavior takes effect, and the new service name will be the service_type + a random number.

OPSAPS-47379 – Spring Framework Upgrade

The Spring Framework used by Cloudera Manager has been upgrade to version 4.3.19.RELEASE.

Fixed Issues in Cloudera Manager 7.3.0

Fixed issues in Cloudera Manager 7.3.0.

Cloudera Bug: OPSAPS-58659: Create a new checkbox in Oozie's Cloudera Manager configuration to control the Callback URL Kerberos enablement

For more information, see https://jira.cloudera.com/browse/DOCS-7797

Cloudera Bug: OPSAPS-56678: SRM client configuration (srm.properties) contains invalid properties

New configuration resolvers added: file, system environment with default. (This change is backward compatible, old configuration works as usual.)

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

When setting up the service the install script failed to properly set the ""fs.defaultFS"" property. Example: core-site.xml:

```
      <property>
        <name>fs.defaultFS/name>
        <value>abfs://bsari-azl@msisan.dfs.core.windows.net/bsar
i-srtest-az</value>
      </property>
```

registry.yaml: fsUrl: "abfs://bsari-azl.dfs.core.windows.net/bsari-srtest-az" Notice: the ""bsari-azl@"" part is missing. Fix: By using sed it can handle the ""@"" character well in replacement.

Cloudera Bug: OPSAPS-53309: Upgrade com.ning:async-http-client:1.9.40 due to CVE

AsyncHttpClient used by Cloudera Manager is upgraded to org.asynchttpclient.async-http-client version 2.12.1.

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

Health State fixed for Schema Registry when having multiple instances

Cloudera Bug: OPSAPS-57411: Configuration for metrics fetching in group or separately

Configurable SMM metrics fetching mode

Cloudera Bug: OPSAPS-57539: Sometimes SMM UI process does not get killed and prevents restarting it

The SMM UI stop script has been improved, so that it will kill the child processes to prevent the SMM UI process from being stuck.

Cloudera Bug: OPSAPS-58661: Increasing default value of ZooKeeper Session Timeout in Kafka

Increasing default value of ZooKeeper Session Timeout in Kafka for 7.1.5 runtime version.

Cloudera Bug: OPSAPS-58708: Failed to log audit event in Ranger for Kafka in AutoTLS enabled cluster

Ranger plugin's audit logging works with non-secure Zookeeper connection while Kafka itself still uses TLS connection to Zookeeper.

Cloudera Bug: OPSAPS-56239: TEZ_JARS classpath directory configuration should not be hardcoded in hive.sh

The parcel root directory had initially been hardcoded in various locations, causing issues if a different path was utilized. The parcels root directory is no longer hardcoded, and is now dynamically set.

Cloudera Bug: OPSAPS-58107: CSD support to configure caching in SMM Authorizer

SMM request processing is sped up by introducing an authorization cache. The default TTL of the cache is 30 seconds and it is configurable in CM. Setting the TTL to 0 disables the cache entirely.

Cloudera Bug: OPSAPS-57745: SMM UI Server failed to start but status in CM still show green

Cloudera Manager now correctly displays role status when the SMM UI process fails/stops.

Cloudera Bug: OPSAPS-58990: SMM and Schema Registry Ranger plugin Solr audits fails with HTTP 403

Fixed SMM Ranger plugin authorization issue with Solr. Audit events can now be logged to Solr.

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-57317: Ranger user cannot send requests to SchemaRegistry

Added user rangerlookup to the default list of users when creating the schemaregistry policy in ranger

Cloudera Bug: OPSAPS-57294: Schema Registry first run fails when multiple Ranger Admin services are configured

Schema Registry startup script now can handle the case when multiple Ranger Admin services are configured.

Cloudera Bug: OPSAPS-57444: SMM throws an error if keystore and private key password are not the same

SMM secure configuration now supports non-matching key and keystore passwords; affects CDH >= 7.2.2 and CDH >= 7.1.4

Cloudera Bug: OPSAPS-58819: Unable to set nullable fields with template import

A restriction was placed to import cluster templates with null values prior to this Cloudera Manager Version. That is causing issues when users import a template generated by a previous CM version. As it used to allow setting null to the configuration field value. With this fix, that restriction has been removed.

Cloudera Bug: OPSAPS-58731: Add CM configurations for raz-s3

Emitting Ranger Raz configs for S3 to HDFS core-site.xml and to RAZ raz-site.xml

Cloudera Bug: OPSAPS-59219: [ranger-raz] Add ranger.raz.service-type.s3.super.users to fix cluster template init failure

Cloudera Bug: OPSAPS-59012: Telemetry Publisher is broken

Telemetry publisher no longer throws ClassDefNotFoundException

Cloudera Bug: OPSAPS-56328: Changing port numbers to non-ephemeral ports

Setting Kafka Connect default ports to be non ephemeral ports.

Cloudera Bug: OPSAPS-58728: Specify JDBC override param in Ranger CSD

Tested only JDBC url override for postgres database type for Ranger CSD supporting CDPD - 7.1.5 installation.

Cloudera Bug: OPSAPS-57410: Add Security related headers to SMM Rest API Server responses

Added Security-Related Headers to SMM Rest API respones: - Strict-Transport-Security - Cache-Control

Cloudera Bug: OPSAPS-57409: Add security related header controls to all Schema Registry responses.

Added the following HTTP headers to ScemaRegistry HTTP responses: -Content-Security-Policy -XSS-Protection -X-Frame options -Content-Type-Options -Cache-control

Cloudera Bug: OPSAPS-58541: Code to disable repeat for HBase schedules

Disabled repeat for HBase replication schedule, similar to Hive3

Cloudera Bug: OPSAPS-58435: Implement remove_peer for HBase replication

Cloudera Bug: OPSAPS-58751: Disable table for HBase replication

Implemented disable table replication for HBase schedules when removing a table from the HBase peer's tableCFs list.

Cloudera Bug: OPSAPS-58473: Implement enable_peer/disable_peer for HBase replication

Implemented enable_peer/disable_peer for HBase replication

Cloudera Bug: OPSAPS-58628: [JUnit testing] Implement enable_peer/disable_peer for HBase replication

Created JUnit tests for OPSAPS-58473: Implement enable_peer/disable_peer for HBase replication

Cloudera Bug: OPSAPS-58539: Redo HBaseReplicationCmdArgs.

Refactored HBaseReplicationCmdArgs

Cloudera Bug: OPSAPS-58542: [hbase][cdh-to-cdp] Proper paramSpec(s) instead of safety valve

Introduced new paramSpec: hbase_replication_auxiliary_info

Cloudera Bug: OPSAPS-56085: Adding a CSD version with new metrics hits staleness check upon upgrading Cloudera Manager

Multiple version compatibility ranges starting within the same major version can now be specified for built-in and CSD metrics. Metric version compatibility ranges that are not composed of one or more full major versions are now honored throughout Cloudera Manager.

Cloudera Bug: OPSAPS-58405: Add GCP support for IDBroker evaluators

GCP IDBroker configs will now appear in core-site.xml

Cloudera Bug: OPSAPS-58617: cdp-proxy topolgy is missing identity-assertion

Added identity-assertion provider into the cdp-proxy Knox topology.

Cloudera Bug: OPSAPS-59184: Incorrect Log4J configuration in Knox's control.sh

Fixed logging issues in Knox IDBroker and corrected log configuration file paths.

Cloudera Bug: OPSAPS-58820: [CDP Public Cloud][7.2.6][RAZ S3] SDX Cluster creation failed, Access Denied for hdfs user

Added hdfs user as superuser for RAZ S3

Cloudera Bug: OPSAPS-58889: HttpFS Safety Valve config for core-site.xml incorrectly gets emitted to hdfs-site.xml

HttpFS Safety Valve config for core-site.xml should now correctly be added to HttpFS core-site.xml.

Cloudera Bug: OPSAPS-54954: CM - Streams Replication Manager's Replication Configs "?" wording goes off page

Streams Replication Manager's Replication Configs help text was wrongly formatted.

Cloudera Bug: OPSAPS-55872: Missing configs in Cruise Control CSD

Added self.healing.goals, hard.goals and anomaly.detection.goals configs. affects: CM >= 7.2.1 and CDH >= 7.2.1, CM >= 7.3.0 and CDH >= 7.1.6

Cloudera Bug: OPSAPS-59143: [Knox] Failed to create new KafkaAdminClient

Fixed properties for Atlas gateway role for proper Atlas Kafka communication.

Cloudera Bug: OPSAPS-58499: Use Impala krpc port for connectivity check

This Jira is related to IMPALA-9180, which remove impala thrift based backend port and use krpc port to construct subscriber_ids.

Cloudera Bug: OPSAPS-56938: Update Spring Data Commons for Security (CM) in 6.3.3 (CVE-2018-1273)

Upgraded to Spring Data Commons 1.13.11

Cloudera Bug: OPSAPS-56854: Update Spring Framework for CM in 7.2.0 (CVE-2018-1270)

Using Spring Framework 4.3.19.RELEASE

Service Pack in Cloudera Manager 7.3.0

You can review the list of CDP Public Cloud hotfixes rolled into Cloudera Manager 7.3.0. This will help you to verify if a hotfix provided to you on a previous CDP Public Cloud release was included in this release.

- OPSAPS-62456 Knox topology redeployment should require changes
  - HOTREQ-911

Known Issues in Cloudera Manager 7.3.0

Learn about the known issues in Cloudera Manager 7.3.0, the impact or changes to the functionality, and the workaround.

Cloudera bug: OPSAPS-59764: Memory leak in the Cloudera Manager agent while downloading the parcels.

When using the M2Crpyto library in the Cloudera Manager agent to download parcels causes a memory leak.

The Cloudera Manager server requires parcels to install a cluster. If any of the URLs of parcels are modified, then the server provides information to all the Cloudera Manager agent processes that are installed on each cluster host.

The Cloudera Manager agent then starts checking for updates regularly by downloading the manifest file that is available under each of the URLs. However, if the URL is invalid or not reachable to download the parcel, then the Cloudera Manager agent shows a 404 error message and the memory of the Cloudera Manager agent process increases due to a memory leak in the file downloader code of the agent.

To prevent this memory leak, ensure all URLs of parcels in Cloudera Manager are reachable. To achieve this, delete all unused and unreachable parcels from the Cloudera Manager parcels page.

Cloudera bug: OPSAPS-63881: When CDP Private Cloud Base is running on RHEL/CentOS/Oracle Linux 8.4, services fail to start because service directories under the /var/lib directory are created with 700 permission instead of 755.

Run the following command on all managed hosts to change the permissions to 755. Run the command for each directory under /var/lib:

```
chmod -R 755 [***path_to_service_dir***]
```

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 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 2021-488: 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)