CDP Private Cloud Base 7.1.5

Release Notes

Date published: 2020-10-09
Date modified: 2020-11-25

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.2.4 Release Notes

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

What's New in Cloudera Manager 7.2.4

New features and changed behavior for Cloudera Manager.

Support for pluggable authentication modules (PAM)

Linux pluggable authentication modules (PAM) are now supported in Cloudera Manager.

Java Keystore Type

Cloudera Manager has added a new configuration "Java Keystore Type" which tells Cloudera Manager the type of keystore type to use when writing and reading keystore and truststore files. This configuration will also be passed down to component services. The value must be a valid keystore format such as "JKS", "PKCS12", or "BCFKS".

SAML signature algorithm update

Users can now select a SAML signature algorithm a SAML message will be signed with. The supported algorithms are RSA-SHA1, RSA-SHA256, RSA-SHA384, RSA-SHA512.

Configuration properties in CSD for SRM Service metric processing

New configuration fields have been added to CM for Streams Replication Manager reliability:

- secondary->primary.metrics.period
- metric.grace
- metric.retention

SMM autoconfiguration of SRM

SMM now auto-configures its SRM connection based on a service dependency, and manual configuration options are removed.

Upgrade of Base Clusters with attached 7.x compute clusters

Upgrades of compute clusters, and of base clusters with one or more data contexts, from Cloudera Runtime 7.x to Cloudera Runtime 7.x are now supported.

Previously, CM could upgrade compute clusters or base-clusters with attached compute clusters and required you to remove all compute clusters and the SDX context, upgrade, and then re-build.

PostgreSQL JDBC driver upgrade

The Postgresql JDBC driver version used by CM has been upgraded to 42.2.14.jre7.

Fixed Issues in Cloudera Manager 7.2.4

Fixed issues in Cloudera Manager 7.2.4.
Cloudera Bug: OPSAPS-58733: [SCM] Unable to upload diagnostic bundles when proxy username is blank

This change fixes the issue of Cloudera Manager being unable to upload the diagnostic bundle via proxy, if a proxy user name is not provided.

Cloudera Bug: OPSAPS-58732: Fix maintenance mode UI

Previously, a host that was commissioned but not in Maintenance Mode could not be taken out of Maintenance Mode via the CM UI. This issue has been fixed.

Cloudera Bug: OPSAPS-58661: SSL-enabled Zookeeper session timeouts in Kafka

The default value for the ZooKeeper session timeout in Kafka has been increased.

Cloudera Bug: OPSAPS-58582: No Java JDK is detected on the host - regression caused by OPSAPS-42725

Previously, setting JAVA_HOME (CM->Hosts->Host Config->JAVA_HOME) to a custom location and restarting Cloudera Manager Agents on the hosts resulted in the configuration error "No Java JDK is detected on the host" under CM->Home->Configuration on Cloudera Manager. This issue has been fixed.

Cloudera Bug: OPSAPS-58488: SMM is missing from ranger users for SchemaRegistry

Fixed an issue where SMM could not connect to Ranger with Cloudera Manager 7.2.4 and Cloudera Runtime 7.1.5.

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

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

Cloudera Bug: OPSAPS-58390: Zookeeper fails to start if trustStore.type is not set

In cCloudera Manager 7.2.4 and later, the keystore type (defaults to JKS) of the keystore and truststore files used for ZooKeeper TLS will be set in the generated zoo.cfg configuration file. If you use a custom keystore format for the KeyStore and TrustStore files on the cluster, change the keystore type in the global CM configuration, following these steps:

- Open Cloudera Manager
- Choose the "Administration" menu
- Choose "Settings" menu
- Search and set the configuration: "Java Keystore Type"

If for any reason you need to set a different keystore type only for ZooKeeper and you need to override the global CM configuration, then add the following configurations to your zoo.cfg safety valves in ZooKeeper configuration (in the example we are defining "JKS" format):

- ssl.keyStore.type=JKS
- ssl.trustStore.type=JKS
- ssl.quorum.keyStore.type=JKS
- ssl.quorum.trustStore.type=JKS

Cloudera Bug: OPSAPS-58374: Some parameters like "zeppelin.ssl.keystore.type" are not being written to zeppelin-site.xml

Fixes an issue where some parameters were not being written to zeppelin-site.xml.

Cloudera Bug: OPSAPS-58319: KafkaEntitiesInfoFetcher does not handle empty response from broker topics endpoint

During startup, Kafka brokers respond with an empty collection on the /api/topics endpoint. If topic names are fetched at this time, Kafka metrics may be wiped. This is due to the empty response not being handled correctly.

Cloudera Bug: OPSAPS-58277: Calls to the third-party ptrace_do library fail on Ubuntu 18

This issue has been fixed. Clusters no longer have to be stopped prior to Cloudera Manager upgrade on Ubuntu 18 when upgrading from Cloudera Manager 6.3.4 or higher, or Cloudera Manager 7.1.5 or higher.

Cloudera Bug: OPSAPS-58242: Improve secondary group lookup performance in supervisord

In environments using AD to manage user groups, service startup could be very slow if there are thousands of groups. This was due to CM agent downloading all the groups to check against the current service user every time a role is started.

The CM agent has been modified to use the system call to download only groups attached to a particular user, which should speed up role startup. This only applies in environments with python 2.7 or later. Environments using python 2.6 (ie Redhat 6 based OS) will fallback to the old behavior.

Cloudera Bug: OPSAPS-58206: HiveServer2 crashing due to the permission issue in loading ozone-site.xml

Fixed the permission issue of loading ozone-site.xml.

Cloudera Bug: OPSAPS-58157: Schema Registry swagger page does not work due to CSP violation

Schema Registry's swagger page now correctly renders and the browser does not report a Content Security Policy violation error.

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

In versions before Cloudera Manager 7.2.3, Schema Registry logs were not displayed in the Cloudera Manager UI. The Schema Registry log format was changed to make it consistent with the log format of other CDP components. Schema Registry Server role logs are now correctly displayed in Cloudera Manager.

Download full Schema Registry logs from Cloudera Manager and analyze logs using an external tool.

Cloudera Bug: OPSAPS-58146: Cloudera Manager doesn't consider version when creating application links

YarnWorkRelatedLinkGenerator was modified to consider the Cloudera Runtime version. For CDH releases the UI1 link will be generated, for CDP and later the UI2.

Cloudera Bug: OPSAPS-58071: CM - Solr Server Log Details page does not show log messages

Newer Solr Server role logs using decimal dots in their timestamps are shown correctly on the corresponding Role Log File page of Cloudera Manager.

Cloudera Bug: OPSAPS-58001: Yarn aggregation job is missing Yarn metric folders because of timezone issues

Fixed an issue where YarnUsageAggregation didn't find directories to aggregate for the IST timezone.

Cloudera Bug: OPSAPS-57942: Fix jobInputCandidateDirs debug logging in YarnUsageAggregator

YarnUsageAggregation candidate directory debug logging is fixed.

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-57907: Kafka metric collector adapter causing too high CPU load

Previously, if a large number of topic partitions are created on a cluster, the Cloudera Manager Agent could generate a high CPU load. This was caused by the Kafka metric collector adapter carrying out excessive regex matching.

The Cloudera Manager Agent no longer generates a high CPU load when fetching Kafka metrics.

Cloudera Bug: OPSAPS-57814: Implement CM upgrade handlers for Oozie 7.1.4 and 7.2.2 (was: 7.1.1 to 7.1.4 upgrade is failing when autoTLS is enabled)

CM will populate the newly introduced ZooKeeper SSL fields for Oozie when AutoTLS is enabled on the Cluster and SSL is enabled for ZooKeeper

Cloudera Bug: OPSAPS-57746: Implement FIPS config param

Cloudera Manager will support running under FIPS compliant mode. It is disabled by default. To enable it add the below to CMF_JAVA_OPTS in /etc/default/cloudera-scm-server of the server host:

-Dcom.cloudera.cmf.fipsMode=true

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

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

Cloudera Bug: OPSAPS-57446: Make 'defaultFS' in Core Configuration service optional, fallback to local disk somewhere

New behavior: Strict validation requiring the Default Filesystem to be specified for the Core Configuration service in base clusters has been removed. Affects all CM versions.

Cloudera Bug: OPSAPS-57268: KDC Connectivity Test fails with AD_USE_SIMPLE_AUTH set to true

KDC Server Connection health check bug fixed, where it showed false alert, when CM was setup with simple auth.

Cloudera Bug: OPSAPS-57099: Selecting "No dependencies" incorrectly selects dependencies

Fixed the issue where selecting no optional dependencies for a new service in the Add Service wizard incorrectly set dependencies.

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 white spaces, due to which the generate missing credentials script in Cloudera Manager fails. This issue has been fixed.

Cloudera Bug: OPSAPS-56577: Customized principle name results in service start failure

Previously, if a Kerberos principal other than "yarn" is configured for the YARN service, then Cloudera Manager will erroneously skip adding the custom principal to the YARN keytab, causing YARN to fail to start due to a Kerberos authentication failure. This also affects Ambari to Cloudera Manager migrations, if Ambari was configured with a principal other than "yarn" for the YARN service. A similar issue affected Hive, when using Hive LLAP.

This issue of the service restart failure while using the custom principal name has been fixed in CM>=7.2.4.

Note: Reset ACLs on YARN every time the yarn principal name is changed.

Cloudera Bug: OPSAPS-56437: Grant ranger hdfs policy on for configured hive group

CDP upgrade will grant Ranger HDFS permission to the Sentry Hive group name configured in HDFS configuration.

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

This issue has been fixed.

Cloudera Bug: OPSAPS-58477: Support custom Kerberos principals for remaining CDP services that don't

This issue has been fixed.

Cloudera Bug: OPSAPS-58847: Remove TLSv1.2 from the list of disabled protocols in ATLAS by default

Atlas TLS protocol excludes changed to TLSv1 and TLSv1.1 instead of earlier TLSv1.2

Cloudera Bug: OPSAPS-58765: Allow customers to configure empty value for CDP Private Cloud repository

This issue has been fixed.

Known Issues in Cloudera Manager 7.2.4

Known issues in CM 7.2.4.

OPSAPS-58679 FIPS cluster install fails at Setup Database step.

Known Issue Description: When setting up a cluster with FIPS + Auto TLS + SSL Postgres enabled, when the Ranger service is added in Cloudera Manager using the Add Service wizard, the database test connection fails with the following error at the Setup Database step:

```
org.postgresql.util.PSQLException: SSL error:
java.security.cert.CertificateException: Certificates do not conf
orm to algorithm constraints
```

Known Issue Workaround: Enable the Use JDBC URL Override property and override the default JDBC URL with the correct JDBC URL.

OPSAPS-57584 FIPS compliance causes flood process to crash.

Known Issue Description: Configuring Cloudera Manager for FIPS compliance requires disabling the flood process.

Known Issue Workaround: When FIPS is enabled, disable the flood process by setting the flood port to 0.

OPSAPS-59511 Cloudera Manager displays invalid services when adding role instances to the Cloudera Management Service.

Known Issue DescriptionCloudera Manager displays the following invalid services when adding a role instance to the Cloudera Management Service: Navigator Audit Server and Navigator Metadata Server. Cloudera Manager also displays the following services that are already installed: Host Monitor, Reports Manager, Service Monitor, and Alert Publisher.

Workaround: Ignore the extra services and continue to add the role instance.

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.

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 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)

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