CDP Private Cloud Base 7.1.1

Release Notes

Date published: 2020-04-10
Date modified:

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.1.1 Release Notes

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

Known Issues in Cloudera Manager 7.1.1

CDPD-4139: A cluster with indices stored on HDFS that was created before enabling TLS, will get the following error message after enabling TLS and starting the cluster:

Will not load SolrCore SOLR_CORE_NAME because it has been replaced due to failover.

Workaround: Recreate the collection after enabling TLS. New collections created after enabling TLS are not affected.

CDPD-10352: Hive on Tez cannot run certain queries on tables stored in encryption zones. This only happens when the KMS connection is SSL encrypted and a self-signed certificate is used. Users may see a SSLHandshakeException in the Hive logs.

Workaround: There are two workarounds:

- Install a self signed SSL certificate into the cacerts file on all hosts.
- Copy the ssl-client.xml file to a directory that is available to all hosts. Then set the the following configuration, tez.aux.uris=path-to-ssl-client.xml in the Hive on Tez Service Environment Advanced Configuration Snippet (Safety Valve).

OPSAPS-56286: If you are running multiple instances of the Schema Registry Server role, an incorrect health state will be displayed for the Schema Registry service even if the underlying role instances are healthy. This is caused by health tests being disabled for the Schema Registry Server due to an invalid configuration.

Workaround:

1. Log in to the Cloudera Manager Server host.
2. Delete or move the Schema Registry CDH 5 compatible CSD from /opt/cloudera/cm/csd/.For example:

```
$ rm /opt/cloudera/cm/csd/SCHEMAREGISTRY_C5-[VERSION_NUMBER]
.jar
```

3. Restart the Cloudera Manager server:

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

CDPD-12060: ID Broker is not supported in Cloudera Manager 7.1.1

OPSAPS-56404: On an upgraded cluster, if the Knox service is added post upgrade and the Ranger Knox plugin is enabled, audits to HDFS for the Knox Ranger plugin fail with permission error on HDFS.

Workaround: When we add Knox service post upgrade, and Ranger Knox plugin is enabled, in the Cloudera Manager Admin Console, go to the Knox service and select Action menuCreate Ranger Knox Plugin Audit Directory, this action should be performed to create the HDFS audit directory.

OPSAPS-56397: When restarting the cluster or performing a cluster upgrade, you may encounter an error when starting a role because there is a pending command running on that role. This can happen if a diagnostic bundle collection is running.

Workaround: If this occurs, you can resume the upgrade once the collection finishes. To avoid this scenario, do not run or schedule diagnostic bundle collection before starting a role or performing a cluster upgrade.

Cloudera Bug: OPSAPS-55785: Upgrade of compute clusters from 7.0.3 -> 7.1.1 is not supported

Upgrades of compute clusters, and of base clusters with one or more associated data contexts, from Cloudera Runtime 7.0 to Cloudera Runtime 7.1 is not supported. The user must first delete their compute clusters, remove any data contexts, upgrade the base cluster and then rebuild.

Cloudera Bug: OPSAPS-55671: Rolling upgrades from Cloudera Runtime 7.0 to Cloudera Runtime 7.1 are not supported

Cluster downtime is required for upgrade.

CDPD-11765, CDPD-11718: Replication Manager cloud replication with Auto-TLS enabled cluster may not function properly due to some functional outage in Hive with cloud storage in CDP Private Cloud Base Auto-TLS enabled cluster.

CDPD-12123: HDFS replication performance is either slowed down or not on the expected lines with CDH/CM 7.1.1. Post-upgrade, queue which the user is running workloads cannot grow beyond the configured capacity till its maximum capacity.

Workaround: Once the cluster is upgraded to CDP Private Cloud Base 7.1.1, user may need to tune yarn.scheduler.capacity.<queuepath>.user-limit-factor to a value greater than 1. This configuration enables the queue usage to grow beyond its configured capacity, till its maximum capacity configured.

OPSAPS-54477 Flume not supported in CDP Private Cloud Base

You must remove the Flume service before upgrading to CDP Private Cloud Base.

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-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.

Action required

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

Knowledge article

For more information about this issue, see the corresponding Knowledge article:

Cloudera Customer Advisory: Cloudera Manager 6.x issue with service role Resume

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

Fixed Issues in Cloudera Manager 7.1.1

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

Cloudera Bug: OPSAPS-56153: [SCM] Diagnostic bundle uploads fail to authenticate with Proxy

Cloudera Manager diagnostic bundle uploads have fixed the 407 authentication exception issue, when a diagnostic bundle was uploaded using a proxy server with basic authentication.

Cloudera Bug: OPSAPS-55810: Cloudera Manager Host Resource page shows invalid Unit/Values for memory for Ozone roles

the Cloudera Manager -> Configuration page showing invalid "Memory Overcommit warnings" with incorrect units is now fixed.

Cloudera Bug: OPSAPS-55542: Modification of IFS leads to unknown result

An issue detected regarding improper handling of duplicates the Cloudera Manager's gen_credentials_ad.sh script is now fixed.

Cloudera Bug: OPSAPS-55870: Installation failed because of health checks

Increased the default number of SCM descriptor fetch attempts from 5 to 10. Furthermore, the sleep interval between fetch attempts will be increased by one additional second per failed attempt.

Cloudera Bug: OPSAPS-56156: Enabling AutoTLS failed on cluster post upgrade

Occasionally, a timeout exception may occur when enabling Auto-TLS or rotating Auto-TLS certificates. The command has been modified to retry up two times in the event of a failure.

Cloudera Bug: OPSAPS-55064: Staleness in Kafka servcie in 7.03 cluster after upgrading Cloudera Manager

Stale Configurations Kafka Stale Configuration Changes in control scripts for Kafka security configuration (related to Ranger and Plain authentication) causing the Kafka configuration to be marked as stale after upgrading to Cloudera Manager 7.1.1. Perform a rolling restart of Kafka.

Cloudera Bug: OPSAPS-56491: Add Kerberos text to Knox CSD description

Warn users while installing Knox service that it is only supported for kerberized clusters

Cloudera Bug: OPSAPS-55143: Disable TLS for agent status server port on RHEL6

Fixed a file descriptor leak in the Cloudera Manager agent when running on Redhat 6 platform with TLS/SSL enabled for Cloudera Manager communications. The fix is to disable TLS/SSL for the Cloudera Manager agent status server port on Redhat 6. Heartbeat protocol and Navigator data (eg

audit events) remain encrypted. 6.2.2 : Fixed a file descriptor leak in the Cloudera Manager agent when running on all platforms with TLS/SSL enabled for Cloudera Manager communications. The fix is to disable TLS/SSL for the Cloudera Manager agent status server port. Heartbeat protocol and Navigator data (eg audit events) remain encrypted. This regresses the behavior to match Cloudera Manager 5.x.

Cloudera Bug: OPSAPS-54951: Cloudera Manager template import fails

Fixed issue where Cloudera Manager gets stuck deploying cluster templates that reference non-CDH parcels.

Cloudera Bug: OPSAPS-56242: External user auth roles become mixed up when posting multiple mappings to API

When creating external role mappings via the /externalUserMappings API endpoint, if multiple mappings are given in the request, then later mappings will erroneously inherit roles specified in preceding mappings, thus granting those users or groups additional privileges than expected. This has been fixed. Note that existing role mappings that have already been created will not be fixed by this change. Cloudera recommendeds you review your existing role mappings in Administration > Users & Roles to correct any inconsistencies.

Cloudera Bug: OPSAPS-55012: AutoTLS should override manual TLS settings in agent

You no longer need to clear TLS configurations from the agent config.ini before enabling Auto-TLS. When enabling Auto-TLS, any existing TLS configurations in config.ini will be overwritten with Auto-TLS-specific configurations.

Cloudera Bug: OPSAPS-54727: HDFS health checks are not visible in the Cloudera Manager Admin Console

HDFS, HBase, MapReduce and Zookeeper health checks are visible again on Cloudera Manager Admin Console.

Cloudera Bug: OPSAPS-54964: Missing client configuration for srm-control

Cloudera Manager can now automatically generate client configuration properties (except security configurations) for srm-control to make it easier to use from the command line.

Cloudera Bug: OPSAPS-56498: Spark compute cluster failing to come up with oozie start failed

Fixed an error where a Virtual Private cluster for Spark started.

Cloudera Bug: OPSAPS-55410: Relax dependency on Kerberos to enable Ranger for Kafka

This fix removes the requirement that Ranger service can only be enabled when Kerberos is on. It enables 2-way SSL configs for Ranger client.

Cloudera Bug: OPSAPS-54635: Service logs of Queuemanager not collected in diagnostic bundles

QueueManager logs are now collected.

Cloudera Bug: OPSAPS-54477: "Missing service handler" error shown when trying to upgrade a cluster with Flume

You must remove Flume before upgrading to CDP Private Cloud Base.

Cloudera Bug: OPSAPS-55168: Server side caching in Schema Registry is now disabled.

Server side caching in Schema Registry is now disabled.

Cloudera Bug: OPSAPS-55881: Host monitor failed to respond

The memory requirements for Cloudera Manager 7.X have increased since Cloudera Manager 6.X. Heap memory size has been increased to 4GB.

Cloudera Bug: OPSAPS-56723: CM - cloudera-manager-installer.bin fails due to missing Postgres

PostgreSQL version 10 is now installed automatically.

Cloudera Bug: OPSAPS-52178: Race condition while starting Impala can prevent profiles from getting sent to Workload Experience Manager

If Impala Daemon is added after Telemetry Publisher, then queries using that Impala Daemon as co-ordinator will not be delivered to Workload XM.

Cloudera Bug: OPSAPS-55390: Need to create HBase tables during Atlas preStart initialization.

Atlas HBase tables are now created in Atlas before installation so that Atlas does not rely on the Ranger HBase plugin to be enabled to create the required tables during upgrades.

Cloudera Bug: OPSAPS-55158: Atlas Default authentication set by defaul to PAM

PAM authentication is now enabled by default for Atlas. File based authentication is disabled by default.

Technical Service Bulletins (TSB)

TSB 2022-507 Certificate expiry issue in CDP

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

What's New in Cloudera Manager 7.1.1

New Supported Upgrades

You can now use Cloudera Manager 7.1.1 to manage the following upgrades:

- CDH 5.13 - 5.16 to CDP Private Cloud Base 7.1

  See Upgrades to CDP Private Cloud Base from CDH.
- CDP Private Cloud Base 7.0 to CDP Private Cloud Base 7.1

  See Upgrading CDH and CDP Private Cloud Base.
- Upgrades from HDP 2.6.5 to CDP Private Cloud Base 7 are supported via Ambari and AM2CM.

  See the Upgrading Ambari and HDP to CDP Private Cloud Base for more information.

See the Upgrade Guide for more information.

New user interface for Upgrade Domains

You can use the Cloudera Manager Admin Console to configure Upgrade Domains in a cluster. See Configuring Upgrade Domains.

Tags in Cloudera Manager

A tag in the context of Cloudera Manager is a name-value pair that is attached to a cluster, service, role or host. Tags allow information to be added to an entity in a very open-ended fashion. A single entity may have any number of tags, as long as each tag name is unique, and tags may be added or removed at any time. All tags appear in diagnostic bundles.

You use the Cloudera Manager API to create, delete, and retrieve tags. See the following endpoints:

- /tags
- /clusters/{clusterName}/tags

Kerberos is configured automatically when adding new services 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. Affects all CDH versions.

Custom cgroup names for Cloudera Manager launched services

This feature adds a new String configuration property named Custom Control Group Resources to the Role configuration Group configurations. The string consists of a list of cgroup references. Each list entry must match the controllers:path as given to the cgexec Linux command-line utility. Any

number of entries can be added to the cgroup list. The entries are space separated. The list entries will be used to launch processes with the matching cgroup configuration. All processes within the Role Configuration Group will use the same cgroup configuration. Cloudera Manager will not attempt to validate the controllers or path. Defining non-existent or incorrect cgroup references will cause the process launch to fail. Setting this new parameter causes any automatic cgroup configurations to be ignored, for example CPU or memory limitations set via other parameters.

New parameter for JVM arguments for all services and roles

There is a new configuration parameter in Cloudera Manager called Extra JVM Arguments for Java-based Services. You can put JVM command-line arguments here, and Cloudera Manager will append those arguments when launching Java-based processes.

Updated Postgres databases

The embedded Postgres Database used by KTS has been upgraded from version 9.3 to 12.1 (when used with a KTS 7.1.1 or later parcel version).

The embedded Postgres Database used for CDP Private Cloud Base Trial installations has been upgraded to version 10.

Cloudera Manager now supports a custom URL for Knox when the alert Publisher generates URLs

Cloudera Manager now supports a custom URL for alerts. In cases where Knox is in use, you can configure the alert to send a valid URL in the alert. The URL can be set under AdministrationSettingsCloudera Manager in the Frontend URL property.

CSD Health tests turn red when there's not enough data to test

In case of insufficient data, Custom Service Descriptor (CSD) health tests will turn grey instead of red.

Cloudera Manager now support configuration of HBase Web UI SPNEGO Authentication

Cloudera Manager now supports secure Web UI with SPNEGO in HBase. To secure the UI, enable the Enable Kerberos Authentication for HTTP Web-Consoles property in Cloudera Manager to secure the Web UIs.

New property for Streams Messaging Manager

A new property, Cloudera Manager Service Monitor Host (cm.metrics.service.monitor.host), has been added to SMM. This property allows you to configure the host of the CM Service Monitor that SMM connects to.

If CM Server and CM Service Monitor are installed on different hosts, you must configure the Cloudera Manager Service Monitor Host and Cloudera Manager Service Monitor Port properties to enable SMM to collect metrics.