Cloudera Manager 7.4.1

Release Notes

Date published: 2020-11-30
Date modified: 2021-04-29

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.4.0 Release Notes

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

What's New in Cloudera Manager 7.4.0

New features and changed behavior for Cloudera Manager 7.4.0.

OPSAPS-59456: Add --shutDownCluster parameter for HBaseGracefulShutdownCommand

Changed the HBase graceful-stop command to include the --shutDownCluster parameter.

OPSAPS-59386: Ability to override JDBC connection string for SchemaRegistry and SMM

The database_jdbc_url_override configuration parameter has been added to Schema Registry and Streams Messaging Manager (SMM). This parameter overrides the JDBC URL of the database and allows you to pass specific parameters if necessary.

OPSAPS-57938: Kafka CSD improvements to automate configuration of Kafka-Atlas hook

Two new configuration fields have been introduced to the Kafka service:

- atlas.metadata.namespace.topic
- atlas.metadata.namespace.client

A new configuration field has been introduced to the Kafka Broker: atlas.audit.enabled. This parameter enables the Kafka -> Atlas auditing plugin. The plugin is autoconfigured and is disabled by default.

Third-party software updates

OPSAPS-59284: The org.apache.commons:commons-compress library is updgrade dto version 1.19 due to a CVE.

The commons-compress library has been upgraded to version 1.19.

OPSAPS-54389: Jython library upgraded to version 2.7.2 due to CVE

The Jython library has been upgraded to version 2.7.2.

Fixed Issues in Cloudera Manager 7.4.0

Fixed issues in Cloudera Manager 7.4.0

Cloudera Bug: OPSAPS-59481: Add default value to ranger.ldap.user.dnpattern parameter for Ranger

A default value has been added to prevent errors when the ranger.ldap.user.dnpattern parameter is not configured.

Cloudera Bug: OPSAPS-59431: Console errors and performance issues on Instances page

Improved the performance of the Select all checkbox on Instances pages for large numbers of instances.

Cloudera Bug: OPSAPS-59247: Add the RAZ s3 cluster name to the Ranger Audit log

The cluster name is now displayed in the Ranger audit log through RAZ.

Cloudera Bug: OPSAPS-56280: Support for cleaning up Ranger service on DataHub deletion

[Improvement] See https://jira.cloudera.com/browse/OPSAPS-56167

Known Issues in Cloudera Manager 7.4.0

Known issues in CM 7.4.0

Cloudera Bug: OPSAPS-59148: Hive on Tez service is marked as stale after Cloudera Manager upgrade

After upgrading Cloudera Manager, Hive On Tez will be marked as stale.

Workaround: If you are affected by this bug, at your next opportunity, restart Hive On Tez. The configuration parameter that will be marked stale is: tez.runtime.shuffle.ssl.enable.

Technical Service Bulletins

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)

Cloudera Manager 7.4.1 Release Notes

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

What's New in Cloudera Manager 7.4.1

New features and changed behavior for Cloudera Manager 7.4.1.

OPSAPS-59410: BasicAuthentication over TLS support for Kafka Metrics

New feature - Added TLS and BasicAuth support to the Kafka Brokers' metrics-related HTTP endpoints. - If both the kafka.http.metrics.ssl.enabled and ssl_enabled configuration properties are enabled, the endpoints will be encrypted via TLS. - If kafka.http.metrics.authentication.enabled is enabled, BasicAuth will be enabled, the username and password will have to be provided in the following properties: kafka.http.metrics.user and kafka.http.metrics.password.

OPSAPS-59446: Kafka client's configuration in Streams Messaging Manager has been simplified

A Kafka clients' security.protocol is auto-configured in Streams Messaging Manager configuration. This change removes the 'Kafka Client Security Protocol' parameter where it was set manually. the Jaas configuration for Kafka Clients can be overridden by using the streams.messaging.manager.kafka.client.sasl.jaas.config property in the Advanced Configuration Snippet for streams-messaging-manager.yaml.

OPSAPS-59530: Service Monitor and Host Monitor scaling improvements

In the CDP Public Cloud environment, the Service Monitor and Host Monitor now adapt their memory settings to improve cluster scaling. This requires the "Automatic Restart Process" to be enabled. (It is enabled by default).

OPSAPS-59895: MapReduce shuffle encryption is enabled by default

MapReduce shuffle SSL is enabled by default if Hadoop SSL is enabled on a cluster.

Fixed Issues in Cloudera Manager 7.4.1

Fixed issues in Cloudera Manager 7.4.1

OPSAPS-59562, OPSAPS-59229: SMM YAML configuration uses plain-text passwords

Previously, Streams Messaging Manager passwords were stored in its configuration file as plain-text. The passwords are now assigned as environment variables.

OPSAPS-59555: HBase validation "Regions In Transition" should be disabled for backup master

Cloudera Manager was trying to execute "Regions in Transition" validations for backup (standby) HBase Masters in highly available deployments. This validation was always unsuccessful, as the related metrics are exposed only by the active HBase Master. This validation is now disabled for the backup HBase Master.

Known Issues in Cloudera Manager 7.4.1

Known issues in CM 7.4.1

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"
```

Technical Service Bulletins

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)