Cloudera Manager 7.11.0

Release Notes

Date published: 2020-11-30
Date modified: 2023-06-26

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.11.0 Release Notes

Known issues, fixed issues and new features for Cloudera Manager 7.11.0.

What's New in Cloudera Manager 7.11.0

New features and changed behavior for Cloudera Manager 7.11.0.

OPSAPS-66992: Cloudera Manager 7.11.0 supports Python 3.8

Cloudera Manager 7.11.0 adds support for using Python 3.8 with the Cloudera Manager agents. Python 3.8 is required for using Cloudera Manager 7.11.0. Cloudera Manager 7.11.0 is supported only on Python 3.8. In this release of Cloudera Manager 7.11.0, the Cloudera Manager Agent requires Python 3.8 instead of Python 2 for the below listed platforms. Python 3.8 is only supported with the following operating systems:

- RHEL 8.4
- RHEL 7.9

OPSAPS-66217: ZooKeeper-less connection support for HBase clients

Clients are required to connect to ZooKeeper to find the location of the RegionServer that hosts the meta table region. Site configuration provides the client a list of ZooKeeper quorum peers and the client uses an embedded ZooKeeper client to query meta location.

New configuration settings are introduced in Cloudera Manager that provide a list of well-known master and backup master locations, and with this information the client can contact any of the master processes directly. Any master in either active or passive state tracks meta location and responds to requests for it with its cached last known location. This removes the dependency of ZooKeeper client from HBase clients and also simplifies the firewall configuration to access HBase.

Fixed Issues in Cloudera Manager 7.11.0

Fixed issues in Cloudera Manager 7.11.0.

OPSAPS-67031: Increase the hive split threads to 64 for AWS and GCP

This fix addresses a performance issue for Ranger Raz with specific cloud providers. As part of this fix, the default value for Hive split processing threads (hive.compute.splits.num.threads) is increased to 64. This change affects only Amazon Web Services (AWS) and Google Cloud Platform (GCP) deployments.

OPSAPS-64882: Upgraded PostgreSQL version

The PostgreSQL version is upgraded from 42.2.24.jre7 to 42.5.1 version to fix CVE issues.

OPSAPS-65870: Log4J 1.2.17 replaced with Reload4J

In this release, Cloudera has replaced all Apache Log4j 1.2.x logging libraries included with Cloudera Manager 7.9.0 with equivalent Reload4j libraries.

OPSAPS-64033: Upgraded Bouncy Castle version

The Bouncy Castle version is upgraded to 1.70 version to fix CVE issues.

OPSAPS-66508: Upgraded commons-codec version

The commons-codec version is upgraded to 1.15 version to fix CVE issues.

OPSAPS-66388: Upgraded commons-fileupload version

The commons-fileupload version is upgraded to 1.5 version to fix CVE issues.

Known Issues in Cloudera Manager 7.11.0

Known issues in Cloudera Manager 7.11.0

OPSAPS-67152: Cloudera Manager does not allow you to update some configuration parameters.

Cloudera Manager does not allow you to set to "0" for the dfs_access_time_precision and dfs_name node_accesstime_precision configuration parameters.

You will not be able to update dfs_access_time_precision and dfs_namenode_accesstime_precision to "0". If you try to enter "0" in these configuration input fields, then the field gets cleared off and results in a validation error: This field is required.

To fix this issue, perform the workaround steps as mentioned in the KB article.

If you need any guidance during this process, contact Cloudera support.

OPSAPS-68629: HDFS HTTPFS GateWay is not able to start with custom krb5.conf location set in Cloudera Manager.

On a cluster with a custom krb5.conf file location configured in Cloudera Manager, HDFS HTTPFS role is not able to start because it does not have the custom Kerberos configuration file setting properly propagated to the service, and therefore it fails with a Kerberos related exception: in threa d "main" java.io.IOException: Unable to initialize WebAppContext at org.apache.hadoop.http.H ttpServer2.start(HttpServer2.java:1240) at org.apache.hadoop.fs.http.server.HttpFSServerWebSer ver.start(HttpFSServerWebServer.java:131) at org.apache.hadoop.fs.http.server.HttpFSServer WebServer.main(HttpFSServerWebServer.java:162) Caused by: java.lang.IllegalArgumentExc eption: Can't get Kerberos realm at org.apache.hadoop.security.HadoopKerberosName.setConfi guration(HadoopKerberosName.java:71) at org.apache.hadoop.security.UserGroupInformation.in itialize(UserGroupInformation.java:329) at org.apache.hadoop.security.UserGroupInformation .setConfiguration(UserGroupInformation.java:380) at org.apache.hadoop.lib.service.hadoop.Fil eSystemAccessService.init(FileSystemAccessService.java:166) at org.apache.hadoop.lib.serve r.BaseService.init(BaseService.java:71) at org.apache.hadoop.lib.server.Server.initServices(Se rver.java:581) at org.apache.hadoop.lib.server.Server.init(Server.java:377) at org.apache.hadoop .fs.http.server.HttpFSServerWebApp.init(HttpFSServerWebApp.java:100) at org.apache.hadoop. lib.servlet.ServerWebApp.contextInitialized(ServerWebApp.java:158) at org.eclipse.jetty.server .handler.ContextHandler.callContextInitialized(ContextHandler.java:1073) at org.eclipse.jetty.se rvlet.ServletContextHandler.callContextInitialized(ServletContextHandler.java:572) at org.ec lipse.jetty.server.handler.ContextHandler.contextInitialized(ContextHandler.java:1002) at org.ecli pse.jetty.servlet.ServletHandler.initialize(ServletHandler.java:765) at org.eclipse.jetty.servlet.Serv letContextHandler.startContext(ServletContextHandler.java:379) at org.eclipse.jetty.webapp.Web AppContext.startWebapp(WebAppContext.java:1449) at org.eclipse.jetty.webapp.WebAppCont ext.startContext(WebAppContext.java:1414) at org.eclipse.jetty.server.handler.ContextHandler.d oStart(ContextHandler.java:916) at org.eclipse.jetty.servlet.ServletContextHandler.doStart(Servlet ContextHandler.java:288) at org.eclipse.jetty.webapp.WebAppContext.doStart(WebAppContext.j ava:524) at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.eclipse.jetty.util.component.ContainerLifeCycle.start(ContainerLifeCycle.java:169) at o rg.eclipse.jetty.util.component.ContainerLifeCycle.doStart(ContainerLifeCycle.java:117) at org .eclipse.jetty.server.handler.AbstractHandler.doStart(AbstractHandler.java:97) at org.eclipse.jett y.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.eclipse.jetty.util.comp onent.ContainerLifeCycle.start(ContainerLifeCycle.java:169) at org.eclipse.jetty.server.Server.sta rt(Server.java:423) at org.eclipse.jetty.util.component.ContainerLifeCycle.doStart(ContainerLi feCycle.java:110) at org.eclipse.jetty.server.handler.AbstractHandler.doStart(AbstractHandler.java :97) at org.eclipse.jetty.server.Server.doStart(Server.java:387) at org.eclipse.jetty.util.component .AbstractLifeCycle.start(AbstractLifeCycle.java:73) at org.apache.hadoop.http.HttpServer2.star t(HttpServer2.java:1218) ... 2 more Caused by: java.lang.IllegalArgumentException: KrbExceptio n: Cannot locate default realm at java.security.jgss/javax.security.auth.kerberos.KerberosPrincipa l.<init>(KerberosPrincipal.java:174) at org.apache.hadoop.security.authentication.util.KerberosU

til.getDefaultRealm(KerberosUtil.java:108) at org.apache.hadoop.security.HadoopKerberosNam e.setConfiguration(HadoopKerberosName.java:69) ...

1. Log in to Cloudera Manager.
2. Select the HDFS service.
3. Select Configurations tab.
4. Search for HttpFS Environment Advanced Configuration Snippet (Safety Valve)
5. Add to or extend the HADOOP_OPTS environment variable with the following value: -Djava.security.krb5.conf=<the custom krb5.conf location>
6. Click Save Changes.

Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.11.0 (Cloudera Runtime 7.2.17)

Common Vulnerabilities and Exposures (CVE) that are fixed in this release.

- CVE-2022-29580
- CVE-2021-36373
- CVE-2021-36374
- CVE-2020-9493
- CVE-2022-23305
- CVE-2018-14721
- CVE-2018-14718
- CVE-2018-14719
- CVE-2018-14720
- CVE-2018-19360
- CVE-2018-19361
- CVE-2018-19362
- CVE-2018-12022
- CVE-2018-12023
- CVE-2022-36364
- CVE-2017-15095
- CVE-2018-5968
- CVE-2022-40146
- CVE-2022-41704
- CVE-2022-42890
- CVE-2022-38398
- CVE-2022-38648
- CVE-2020-26939
- CVE-2020-13955
- CVE-2021-4125
- CVE-2022-31129
- CVE-2018-11792
- CVE-2021-28131
- CVE-2018-11785
- CVE-2022-21724
- CVE-2022-31197
- CVE-2022-41946
- CVE-2021-27905
- CVE-2021-44548
- CVE-2021-29943

- CVE-2020-13941
- CVE-2017-3163
- CVE-2017-3164
- CVE-2018-1308
- CVE-2019-12401
- CVE-2019-0193
- CVE-2015-8795
- CVE-2015-8796
- CVE-2015-8797
- CVE-2018-11802
- CVE-2020-5421
- CVE-2022-22978
- CVE-2021-22112
- CVE-2022-22976
- CVE-2022-40152
- CVE-2022-40151
- CVE-2022-41966
- CVE-2020-10683
- CVE-2014-0229
- CVE-2014-3627
- CVE-2013-4221
- CVE-2013-4271
- CVE-2017-14868
- CVE-2017-14949
- CVE-2014-1868
- CVE-2017-5637
- CVE-2021-37533
- CVE-2022-25168
- CVE-2021-33036
- CVE-2022-37865
- CVE-2022-37866
- CVE-2013-2035
- CVE-2021-33813
- CVE-2022-40149
- CVE-2022-40150
- CVE-2022-45685
- CVE-2022-45693
- CVE-2017-7657
- CVE-2017-7658
- CVE-2017-7656
- CVE-2017-9735
- CVE-2020-27216
- CVE-2019-10247
- CVE-2019-10241
- CVE-2016-5725
- CVE-2022-36033
- CVE-2018-1320
- CVE-2019-0205
- CVE-2019-0210
- CVE-2018-11798

- CVE-2016-2402
- CVE-2022-26336
- CVE-2022-38752
- CVE-2022-41854
- CVE-2017-8028
- CVE-2018-1258
- CVE-2020-11988

Cumulative hotfixes

You can review the list of cumulative hotfixes that were shipped for Cloudera Manager 7.11.0 release.

Cloudera Manager 7.11.0-h12

Know more about the Cloudera Manager 7.11.0-h12 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.1200 service pack release.

This cumulative hotfix was released on June 4, 2025.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.0-h12 (version: 7.11.0-h12-66302443):

OPSAPS-71566: The polling logic of RemoteCmdWork goes down if the remote Cloudera Manager goes down

When the remote Cloudera Manager goes down or when there are network failures, the RemoteCmdWork stops to poll. To ensure that the daemon continues to poll even when there are network failures or if the Cloudera Manager goes down, you can set the remote_cmd_network_failure_max_poll_count=*[*** ENTER REMOTE EXECUTOR MAX POLL COUNT***]* parameter on the Cloudera Manager Administration Settings page. Note that the actual timeout is provided by a piecewise constant function (step function) where the breakpoints are: 1 through 11 is 5 seconds, 12 through 17 is 1 minute, 18 through 35 is 2 minutes, 36 through 53 is 5 minutes, 54 through 74 is 8 minutes, 75 through 104 is 15 minutes, and so on. Therefore when you enter 1, the polling continues for 5 seconds after the Cloudera Manager goes down or after a network failure. Similarly when you set it 75, the polling continues for 15 minutes.

OPSAPS-72978: The getUsersFromRanger API parameter truncates the user list after 200 items

The Cloudera Manager API endpoint v58/clusters/*[***CLUSTER***]*/services/*[***SERVICE***]*/commands/getUsersFromRanger no longer truncates the list of returned users at 200 items.

OPSAPS-73529: Backported the ability to disable ZooKeeper clientPort by allowing zero value

The user is now able to set 0 value (disable) to ZooKeeper's clientPort setting.

The repositories for Cloudera Manager 7.11.0-h12 are listed in the following table:

Table 1: Cloudera Manager 7.11.0-h12

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h12-66302443/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h12-66302443/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h12-66302443/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h12-66302443/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.11.0-h11

Know more about the Cloudera Manager 7.11.0-h11 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.1100 service pack release.

This cumulative hotfix was released on April 21, 2025.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.0-h11 (version: 7.11.0-h11-64662076):

OPSAPS-71566: The polling logic of RemoteCmdWork goes down if the remote Cloudera Manager goes down

When the remote Cloudera Manager goes down or when there are network failures, the RemoteCmdWork stops to poll. To ensure that the daemon continues to poll even when there are network failures or if the Cloudera Manager goes down, you can set the remote_cmd_network_failure_max_poll_count=*[*** ENTER REMOTE EXECUTOR MAX POLL COUNT***]* parameter on the Cloudera Manager Administration Settings page. Note that the actual timeout is provided by a piecewise constant function (step function) where the breakpoints are: 1 through 11 is 5 seconds, 12 through 17 is 1 minute, 18 through 35 is 2 minutes, 36 through 53 is 5 minutes, 54 through 74 is 8 minutes, 75 through 104 is 15 minutes, and so on. Therefore when you enter 1, the polling continues for 5 seconds after the Cloudera Manager goes down or after a network failure. Similarly when you set it 75, the polling continues for 15 minutes.

The repositories for Cloudera Manager 7.11.0-h11 are listed in the following table:

Table 2: Cloudera Manager 7.11.0-h11

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h11-64662076/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h11-64662076/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h11-64662076/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h11-64662076/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.11.0-h10

Know more about the Cloudera Manager 7.11.0-h10 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.1000 service pack release.

This cumulative hotfix was released on March 13, 2025.

There are no Fixed issues for Cloudera Manager 7.11.0-h10 (version: 7.11.0-h10-63131628) in Cloudera Runtime 7.2.17.1000 service pack release.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

The repositories for Cloudera Manager 7.11.0-h10 are listed in the following table:

Table 3: Cloudera Manager 7.11.0-h10

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h10-63131628/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h10-63131628/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h10-63131628/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h10-63131628/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.11.0-h9

Know more about the Cloudera Manager 7.11.0-h9 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.900 service pack release.

This cumulative hotfix was released on February 5, 2025.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.0-h9 (version: 7.11.0-h9-61803386):
OPSAPS-72254: FIPS Failed to upload Spark example jar to HDFS in cluster mode

Fixed an issue with deploying the Spark 3 Client Advanced Configuration Snippet (Safety Valve) for spark3-conf/spark-env.sh.

For more information, see Added a new Cloudera Manager configuration parameter spark_pyspark_executable_path to Livy for Spark 3.

OPSAPS-71647: Ozone replication fails for incompatible source and target Cloudera Manager versions during the payload serialization operation

Replication Manager now recognizes and annotates the required fields during the payload serialization operation. For the list of unsupported Cloudera Manager versions that do not have this fix, see Preparing clusters to replicate Ozone data.

OPSAPS-71659: Ranger replication policy fails because of incorrect source to destination service name mapping

Ranger replication policy failed because of incorrect source to destination service name mapping format during the transform step. This issue is fixed.

New features and changed behavior for Cloudera Manager 7.11.0-h9 (version: 7.11.0-h9-61803386):
Added a new Cloudera Manager configuration parameter spark_pyspark_executable_path to Livy for Spark 3.

In Cloudera Manager Agent 7.13.1 and higher versions, a new Cloudera Manager configuration parameter spark_pyspark_executable_path is added to Livy for Spark 3 service.

The value of spark_pyspark_executable_path for Livy must sync with the value of the Spark 3 service's spark_pyspark_executable_path parameter in Cloudera Manager.

Important:

If the PYSPARK_PYTHON/PYSPARK_DRIVER_PYTHON environment variables are not set in spark-env.sh, then the default value of these variables will be the value of the spark_pyspark_executable_path Cloudera Manager property.

The default value of spark_pyspark_executable_path is /opt/cloudera/cm-agent/bin/python.

Summary: The Livy proxy user is taken from Livy for Spark 3's configuration.

Previous behavior:

The custom Kerberos principal configuration was updated via the Livy service.

New behavior:

The Livy proxy user is taken from Livy for Spark 3's configuration, as the Livy service has been replaced with Livy for Spark3 in Cloudera Private Cloud Public Cloud version 7.3.1.

The repositories for Cloudera Manager 7.11.0-h9 are listed in the following table:

Table 4: Cloudera Manager 7.11.0-h9

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h9-61803386/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h9-61803386/redhat8/yum/cloudera-manager.repo`

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h9-61803386/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h9-61803386/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.11.0-h8

Know more about the Cloudera Manager 7.11.0-h8 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.800 service pack release.

This cumulative hotfix was released on October 31, 2024.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.0-h8 (version: 7.11.0-h8-57918262):

OPSAPS-71005: RemoteCmdWork is using a singlethreaded executor

By default, Replication Manager runs the remote commands for a replication policy through a single-thread executor. You can search and enable the enable_multithreaded_remote_cmd_executor property in the target Cloudera Manager Administration Settings page to run future replication

policies through the multi-threaded executor. This action improves the processing performance of the replication workloads.

Additionally, you can also change the multithreaded_remote_cmd_executor_max_threads and multithreaded_remote_cmd_executor_keepalive_time properties to fine-tune the replication policy performance.

OPSAPS-69996: HBase snapshot creation in Cloudera Manager works as expected

During the HBase snapshot creation process, the snapshot create command sometimes tries to create the same snapshot twice because of an unhandled OptimisticLockException during the database write operation. This resulted in intermittent HBase snapshot creation failures. The issue is fixed now.

OPSAPS-66459: Enable concurrent Hive external table replication policies with the same cloud root

When the HIVE_ALLOW_CONCURRENT_REPLICATION_WITH_SAME_CLOUD_ROOT_PATH feature flag is enabled, Replication Manager can run two or more Hive external table replication policies with the same cloud root path concurrently.

For example, if two Hive external table replication policies have s3a://bucket/hive/data as the cloud root path and the feature flag is enabled, Replication manager can run these policies concurrently.

By default, this feature flag is disabled. To enable the feature flag, contact your Cloudera account team.

OPSAPS-69782: HBase replication policies work as expected when the peer Cloudera Manager's API version is higher than the local cluster's API version

HBase replication using HBase replication policies between two Data Hubs/COD clusters would fail if all the following conditions are true:

- The destination Data Hub/COD cluster's Cloudera Manager version is 7.9.0-h7 through 7.9.0-h9 or 7.11.0-h2 through 7.11.0-h4, or 7.12.0.0.
- The source Data Hub/COD cluster's Cloudera Manager major version is higher than the destination cluster's Cloudera Manager major version.
- The Initial Snapshot option is chosen during the HBase replication policy creation process and/or the source cluster is already participating in another HBase replication setup as a source or destination with a third cluster.

This issue is resolved.

The repositories for Cloudera Manager 7.11.0-h8 are listed in the following table:

Table 5: Cloudera Manager 7.11.0-h8

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h8-57918262/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h8-57918262/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h8-57918262/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h8-57918262/redhat7/yum/cloudera-manager.repo`

Cloudera Manager 7.11.0-h7

Know more about the Cloudera Manager 7.11.0-h7 hotfix version which is a corresponding Cloudera Manager hotfix version for Cloudera Runtime 7.2.17.700 service pack release.

This cumulative hotfix was released on September 17, 2024.

Note: Contact Cloudera Support for questions related to any specific hotfixes.

New features and changed behavior for Cloudera Manager 7.11.0-h7 (version: 7.11.0-h7-55447511):
OPSAPS-69495: Implemented support for Ranger Plugin Secure Auditing in Solr using Zookeeper.

Support has been added for Ranger plugin secure auditing in Solr by using ZooKeeper.

OPSAPS-70320: Added Zookeeper SSL connection support for Ranger & Ranger Raz

Support has been added for ZooKeeper SSL connection for Ranger and Ranger RAZ.

Following are the list of fixed issues that were shipped for Cloudera Manager 7.11.0-h7 (version: 7.11.0-h7-55447511):
OPSAPS-70859: Ranger metrics APIs were not working on FedRAMP cluster

On FedRAMP HA cloud cluster, Ranger metrics APIs were not working.This issue is fixed now by introducing new Ranger configurations.

This issue is fixed now by introducing new Ranger configurations.

The repositories for Cloudera Manager 7.11.0-h7 are listed in the following table:

Table 6: Cloudera Manager 7.11.0-h7

Repository Type	Repository Location

RHEL 8 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h7-55447511/redhat8/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h7-55447511/redhat8/yum/cloudera-manager.repo`

Repository Type	Repository Location

RHEL 7 Compatible	Repository:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h7-55447511/redhat7/yum`
	Repository File:
	`https://USERNAME:PASSWORD@archive.cloudera.com/p/cm-public/7.11.0-h7-55447511/redhat7/yum/cloudera-manager.repo`