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