

Cloudera Runtime 7.2.11

Release Notes

Date published: 2021-09-08

Date modified:

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

CVE-2021-45105 & CVE-2021-44832 Remediation for 7.2.11.....	6
CVE-2021-4428 Remediation for 7.2.11.....	6
Overview.....	6
Cloudera Runtime Component Versions.....	6
Using the Cloudera Runtime Maven repository.....	8
RUNTIME 7.2.11.0-233.....	8
What's New In Cloudera Runtime 7.2.11.....	28
What's New in Apache HBase.....	28
What's New in Apache Hive.....	28
What's New in Apache Impala.....	28
What's New in Apache Kafka.....	29
What's New in Apache Kudu.....	29
What's New in Apache Phoenix.....	30
What's New in Schema Registry.....	30
What's New in Cloudera Search.....	31
What's New in Apache Spark.....	31
What's New in Sqoop.....	31
What's new in Streams Messaging Manager.....	31
What's New in Streams Replication Manager.....	32
What's New in Apache Hadoop YARN.....	32
Unaffected Components in this release.....	34
Fixed Issues In Cloudera Runtime 7.2.11.....	35
Fixed Issues in Atlas.....	35
Fixed Issues in Avro.....	35
Fixed Issues in Cloud Connectors.....	35
Fixed issues in Cruise Control.....	36
Fixed issues in Data Analytics Studio.....	36
Fixed Issues in Apache Hadoop.....	36
Fixed Issues in HBase.....	36
Fixed Issues in HDFS.....	37
Fixed Issues in Apache Hive.....	37
Fixed Issues in Hive Warehouse Connector.....	38
Fixed Issues in Hue.....	38
Fixed Issues in Apache Impala.....	38
Fixed Issues in Apache Kafka.....	39
Fixed Issues in Apache Knox.....	39
Fixed Issues in Apache Kudu.....	40

Fixed Issues in Apache Oozie.....	40
Fixed Issues in Phoenix.....	41
Fixed Issues in Parquet.....	41
Fixed Issues in Apache Ranger.....	41
Fixed Issues in Schema Registry.....	42
Fixed Issues in Apache Solr.....	43
Fixed Issues in Spark.....	43
Fixed Issues in Apache Sqoop.....	44
Fixed Issues in Streams Messaging Manager.....	44
Fixed Issues in Streams Replication Manager.....	44
Fixed Issues in Apache Hadoop YARN.....	45
Fixed Issues in Zeppelin.....	45
Fixed Issues in Apache ZooKeeper.....	47
Fixed Issues In Cloudera Runtime 7.2.11.9.....	47
Fixed Issues In Cloudera Runtime 7.2.11.10.....	47
Fixed Issues In Cloudera Runtime 7.2.11.11.....	47
Fixed Issues In Cloudera Runtime 7.2.11.12.....	48
Fixed Issues In Cloudera Runtime 7.2.11.13.....	48
Service Pack in Cloudera Runtime 7.2.11.....	48
Known Issues In Cloudera Runtime 7.2.11.....	48
Known Issues in Apache Atlas.....	48
Known Issues in Apache Avro.....	52
Known Issues in Data Analytics Studio.....	52
Known Issues in Apache HBase.....	53
Known Issues in HDFS.....	54
Known Issues in Apache Hive.....	55
Known Issues in Hue.....	58
Known Issues in Apache Impala.....	60
Known Issues in Apache Kafka.....	64
Known Issues in Apache Knox.....	66
Known Issues in Apache Kudu.....	66
Known Issues in Apache Oozie.....	66
Known Issues in Apache Phoenix.....	67
Known Issues in Apache Ranger.....	67
Known Issues in Schema Registry.....	68
Known Issues in Cloudera Search.....	68
Known Issues in Apache Spark.....	72
Known Issues for Apache Sqoop.....	72
Known issues in Streams Messaging Manager.....	73
Known Issues in Streams Replication Manager.....	74
Known Issues in MapReduce and YARN.....	77
Known Issues in Apache Zeppelin.....	82

Known Issues in Apache ZooKeeper.....	82
Behavioral Changes In Cloudera Runtime 7.2.11.....	82
Behavioral Changes in Cloudera Search.....	83
Behavioral Changes in Apache Phoenix.....	83
Deprecation Notices In Cloudera Runtime 7.2.11.....	83
Deprecation notices in Apache Kudu.....	84
Deprecation Notices for Apache Kafka.....	84
Deprecation Notices in Apache HBase.....	85

CVE-2021-45105 & CVE-2021-44832 Remediation for 7.2.11

Learn about the CVE-2021-45105 & CVE-2021-44832 Remediation for 7.2.11.

On February 1, 2022, Cloudera released a hotfix to Public Cloud Runtime version 7.2.11. It addresses the CVE and other vulnerability concerns as listed below:

- [CVE-2021-45105](#) which affects Apache Log4j2 versions from 2.0-beta9 to 2.16.0, excluding 2.12.3
- [CVE-2021-44832](#) which affects Apache Log4j2 versions from 2.0-alpha7 to 2.17.0, excluding 2.3.2 and 2.12.4

All new CDP environments with Data Lakes using Runtime 7.2.11 that are registered after this hotfix has been released include the vulnerability fix.

You should upgrade your CDP services running Runtime version 7.2.11 so that they include the hotfix. You can update your existing Data Lake and Data Hubs by performing a maintenance upgrade. You should first upgrade the Data Lake and then upgrade all the Data Hubs that are using the Data Lake. The maintenance upgrade is not supported for RAZ-enabled environments. Refer to [Data Lake upgrade](#) and [Data Hub upgrade](#) documentation.

CVE-2021-4428 Remediation for 7.2.11

You can learn more about the CVE-2021-4428 Remediation for 7.2.11.

On January 3, 2022, Cloudera released Public Cloud runtime version 7.2.11_4. It addresses 2 CVEs and other vulnerability concerns as listed below.

- [CVE-2021-44228](#) which affects Apache Log4j2 versions 2.0 through 2.14.1.
- [CVE-2021-45046](#) which affects Apache Log4j2 version 2.15.0
- [LOGBACK-1591](#) which affects logback versions <= 1.2.7

Cloudera urges all customers on the runtime version 7.2.11 (for Datalake or Datahub) to upgrade their services to the latest version.

Overview

You can review the Release Notes of Cloudera Runtime 7.2.11 for release-specific information related to new features and improvements, bug fixes, deprecated features and components, known issues, and changed features that can affect product behavior.

Cloudera Runtime Component Versions

You must be familiar with the versions of all the components in the Cloudera Runtime 7.2.11 distribution to ensure compatibility of these components with other applications. You must also be aware of the available Technical Preview components and use them only in a testing environment.

Apache Components

Component	Version
Apache Arrow	0.11.1.7.2.11.0-233
Apache Atlas	2.1.0.7.2.11.0-233
Apache Calcite	1.21.0.7.2.11.0-233
Apache Avro	1.8.2.7.2.11.0-233

Component	Version
Apache Hadoop (Includes YARN and HDFS)	3.1.1.7.2.11.0-233
Apache HBase	2.2.6.7.2.11.0-233
Apache Hive	3.1.3000.7.2.11.0-233
Apache Impala	4.0.0.7.2.11.0-233
Apache Kafka	2.5.0.7.2.11.0-233
Apache Knox	1.3.0.7.2.11.0-233
Apache Kudu	1.15.0.7.2.11.0-233
Apache Livy	0.6.0.7.2.11.0-233
Apache MapReduce	3.1.1.7.2.11.0-233
Apache NiFi	1.13.2.7.2.11.0-233
Apache NiFi Registry	0.8.0.7.2.11.0-233
Apache Oozie	5.1.0.7.2.11.0-233
Apache ORC	1.5.1.7.2.11.0-233
Apache Parquet	1.10.99.7.2.11.0-233
Apache Phoenix	5.1.1.7.2.11.0-233
Apache Ranger	2.1.0.7.2.11.0-233
Apache Solr	8.4.1.7.2.11.0-233
Apache Spark	2.4.7.7.2.11.0-233
Apache Sqoop	1.4.7.7.2.11.0-233
Apache Tez	0.9.1.7.2.11.0-233
Apache Zeppelin	0.8.2.7.2.11.0-233
Apache ZooKeeper	3.5.5.7.2.11.0-233

Other Components

Component	Version
Data Analytics Studio	1.4.2.7.2.11.0-233
GCS Connector	2.1.2.7.2.11.0-233
HBase Indexer	1.5.0.7.2.11.0-233
Hue	4.5.0.7.2.11.0-233
Search	1.0.0.7.2.11.0-233
Schema Registry	0.10.0.7.2.11.0-233
Streams Messaging Manager	2.1.0.7.2.11.0-233
Streams Replication Manager	1.0.0.7.2.11.0-233

Connectors and Encryption Components

Component	Version
HBase connectors	1.0.0.7.2.11.0-233
Hive Meta Store (HMS)	1.0.0.7.2.11.0-233
Hive on Tez	1.0.0.7.2.11.0-233
Hive Warehouse Connector	1.0.0.7.2.11.0-233

Component	Version
Spark Atlas Connector	0.1.0.7.2.11.0-233
Spark Schema Registry	1.1.0.7.2.11.0-233

Using the Cloudera Runtime Maven repository

Information about using Maven to build applications with Cloudera Runtime components.

If you want to build applications or tools for use with Cloudera Runtime components and you are using Maven or Ivy for dependency management, you can pull the Cloudera Runtime artifacts from the Cloudera Maven repository. The repository is available at <https://repository.cloudera.com/artifactory/cloudera-repos/>.



Important: When you build an application JAR, do not include CDH JARs, because they are already provided. If you do, upgrading CDH can break your application. To avoid this situation, set the Maven dependency scope to provided. If you have already built applications which include the CDH JARs, update the dependency to set scope to provided and recompile.

The following is a sample POM (pom.xml) file:

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/maven-v4_0_0.xsd">
  <repositories>
    <repository>
      <id>cloudera</id>
      <url>https://repository.cloudera.com/artifactory/cloudera-repos/</url>
    </repository>
  </repositories>
</project>
```

RUNTIME 7.2.11.0-233

The following table lists the project name, groupId, artifactId, and version required to access each RUNTIME artifact.

Project	groupId	artifactId	version
Apache Accumulo	org.apache.accumulo	accumulo-core	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-examples-simple	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-fate	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-gc	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-master	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-minicluster	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-monitor	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-proxy	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-server-base	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-shell	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-start	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-test	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-trace	1.7.0.7.2.11.0-233
	org.apache.accumulo	accumulo-tracer	1.7.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.accumulo	accumulo-tserver	1.7.0.7.2.11.0-233
Apache Atlas	org.apache.atlas	atlas-authorization	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-aws-s3-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-azure-adls-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-classification-updater	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-client-common	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-client-v1	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-client-v2	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-common	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-distro	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-docs	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-graphdb-api	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-graphdb-common	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-graphdb-janus	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-index-repair-tool	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-intg	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-janusgraph-hbase2	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-notification	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-plugin-classloader	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-repository	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-server-api	2.1.0.7.2.11.0-233
	org.apache.atlas	atlas-testtools	2.1.0.7.2.11.0-233
	org.apache.atlas	hbase-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	hbase-bridge-shim	2.1.0.7.2.11.0-233
	org.apache.atlas	hbase-testing-util	2.1.0.7.2.11.0-233
	org.apache.atlas	hdfs-model	2.1.0.7.2.11.0-233
	org.apache.atlas	hive-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	hive-bridge-shim	2.1.0.7.2.11.0-233
	org.apache.atlas	impala-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	impala-bridge-shim	2.1.0.7.2.11.0-233
	org.apache.atlas	impala-hook-api	2.1.0.7.2.11.0-233
	org.apache.atlas	kafka-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	kafka-bridge-shim	2.1.0.7.2.11.0-233
	org.apache.atlas	navigator-to-atlas	2.1.0.7.2.11.0-233
	org.apache.atlas	sample-app	2.1.0.7.2.11.0-233
	org.apache.atlas	sqoop-bridge	2.1.0.7.2.11.0-233
	org.apache.atlas	sqoop-bridge-shim	2.1.0.7.2.11.0-233
Apache Avro	org.apache.avro	avro	1.8.2.7.2.11.0-233
	org.apache.avro	avro-compiler	1.8.2.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.avro	avro-ipc	1.8.2.7.2.11.0-233
	org.apache.avro	avro-mapred	1.8.2.7.2.11.0-233
	org.apache.avro	avro-maven-plugin	1.8.2.7.2.11.0-233
	org.apache.avro	avro-protobuf	1.8.2.7.2.11.0-233
	org.apache.avro	avro-service-archetype	1.8.2.7.2.11.0-233
	org.apache.avro	avro-thrift	1.8.2.7.2.11.0-233
	org.apache.avro	avro-tools	1.8.2.7.2.11.0-233
	org.apache.avro	trevni-avro	1.8.2.7.2.11.0-233
	org.apache.avro	trevni-core	1.8.2.7.2.11.0-233
Apache Calcite	org.apache.calcite	calcite-babel	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-core	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-druid	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-kafka	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-linq4j	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-server	1.21.0.7.2.11.0-233
	org.apache.calcite	calcite-ubenchmark	1.21.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-core	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-metrics	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-metrics-dropwizardmetrics	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-noop-driver	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-server	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-standalone-server	1.16.0.7.2.11.0-233
	org.apache.calcite.avatica	avatica-tck	1.16.0.7.2.11.0-233
Apache Crunch	org.apache.crunch	crunch-archetype	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-contrib	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-core	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-examples	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-hbase	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-hive	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-scrunch	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-spark	0.11.0.7.2.11.0-233
	org.apache.crunch	crunch-test	0.11.0.7.2.11.0-233
Apache Druid	org.apache.druid	druid-aws-common	0.17.1.7.2.11.0-233
	org.apache.druid	druid-benchmarks	0.17.1.7.2.11.0-233
	org.apache.druid	druid-console	0.17.1.7.2.11.0-233
	org.apache.druid	druid-core	0.17.1.7.2.11.0-233
	org.apache.druid	druid-gcp-common	0.17.1.7.2.11.0-233
	org.apache.druid	druid-hll	0.17.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.druid.extensions	druid-scheduler-average-query	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-emitter	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-cache	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-sketch	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-extensions	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-min-max	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-columns	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-logger	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-contrib	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-view-maintenance	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-view-selection	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-data-storage	0.17.1.7.2.11.0-233
	org.apache.druid.extensions	druid-scheduler-contrib	0.17.1.7.2.11.0-233
GCS Connector	com.google.cloud.bigtable	gcs-connector	2.1.2.7.2.11.0-233
	com.google.cloud.bigtable	gcs-connector	2.1.2.7.2.11.0-233
Apache Hadoop	org.apache.hadoop	hadoop-aliyun	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-annotations	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-archive-logs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-archives	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-assemblies	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-auth	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-aws	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-azure	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-azure-datalake	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-build-tools	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-client	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-client-api	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-client-integration-tests	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-client-minicluster	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-client-runtime	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-cloud-storage	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-common	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-datajoin	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-distcp	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-extras	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-fs2img	3.1.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hadoop	hadoop-gridmix	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-client	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-common	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-config	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-container-service	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-docs	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-hadoop-dependency-client	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-hadoop-dependency-server	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-hadoop-dependency-test	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-interface-admin	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-interface-client	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-interface-server	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-server-framework	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-server-scm	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-test-utils	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdds-tools	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs-client	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs-httpfs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs-native-client	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs-nfs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-hdfs-rbf	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-kafka	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-kms	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-app	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-common	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-core	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-hs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-hs-plugins	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-jobclient	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-nativetask	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-shuffle	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-client-uploader	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-mapreduce-examples	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-maven-plugins	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-minicluster	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-minikdc	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-nfs	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-openstack	3.1.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hadoop	hadoop-ozone-client	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-common	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-csi	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-datanode	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-dist	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-filesystem	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-filesystem-common	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-filesystem-hadoop2	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-filesystem-hadoop3	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-filesystem-shaded	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-insight	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-integration-test	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-interface-client	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-interface-storage	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-network-tests	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-ozone-manager	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-recon	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-reconcodegen	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-s3gateway	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-ozone-tools	1.1.0.7.2.11.0-233
	org.apache.hadoop	hadoop-resourceestimator	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-rumen	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-sls	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-streaming	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-tools-dist	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-api	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-applications-distributedshell	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-applications-unmanaged-am-launcher	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-client	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-common	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-registry	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-applicationhistoryservice	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-common	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-nodemanager	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-resourcemanager	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-router	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-sharedcachemanager	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-tests	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-timeline-pluginstorage	3.1.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hadoop	hadoop-yarn-server-timelineservice	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-timelineservice-hbase-client	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-timelineservice-hbase-common	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-timelineservice-hbase-server-2	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-timelineservice-hbase-tests	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-server-web-proxy	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-services-api	3.1.1.7.2.11.0-233
	org.apache.hadoop	hadoop-yarn-services-core	3.1.1.7.2.11.0-233
	org.apache.hadoop	mini-chaos-tests	1.1.0.7.2.11.0-233
Apache HBase	org.apache.hbase	hbase-annotations	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-checkstyle	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-client	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-client-project	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-common	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-endpoint	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-examples	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-external-blockcache	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-hadoop-compat	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-hadoop2-compat	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-hbtop	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-http	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-it	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-mapreduce	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-metrics	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-metrics-api	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-procedure	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-protocol	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-protocol-shaded	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-replication	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-resource-bundle	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-rest	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-rsgroup	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-server	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-client	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-client-byo-hadoop	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-client-project	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-mapreduce	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-testing-util	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-shaded-testing-util-tester	2.2.6.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hbase	hbase-shell	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-testing-util	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-thrift	2.2.6.7.2.11.0-233
	org.apache.hbase	hbase-zookeeper	2.2.6.7.2.11.0-233
	org.apache.hbase.contrib	hbase-kafka-model	1.0.0.7.2.11.0-233
	org.apache.hbase.contrib	hbase-kafka-proxy	1.0.0.7.2.11.0-233
	org.apache.hbase.contrib	hbase-spark	1.0.0.7.2.11.0-233
	org.apache.hbase.contrib	hbase-spark-it	1.0.0.7.2.11.0-233
	org.apache.hbase.contrib	hbase-spark-protocol	1.0.0.7.2.11.0-233
	org.apache.hbase.contrib	hbase-spark-protocol-shaded	1.0.0.7.2.11.0-233
	org.apache.hbase.filesystem	hbase-hdfs-impl	1.0.0.7.2.11.0-233
	org.apache.hbase.filesystem	hbase-hdfs	1.0.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-htrace	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-gson	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-jersey	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-jetty	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-miscellaneous	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-netty	3.5.0.7.2.11.0-233
	org.apache.hbase.thriftparty	hbase-tnoop-shaded-protobuf	3.5.0.7.2.11.0-233
Apache Hive	org.apache.hive	catalogd-unit	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-accumulo-handler	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-beeline	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-blobstore	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-classification	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-cli	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-common	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-contrib	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-druid-handler	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-exec	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-hbase-handler	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-hcatalog-it-unit	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-hplsql	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-impala	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-custom-serde	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-druid	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-impala	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-minikdc	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-qfile	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-qfile-accumulo	3.1.3000.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hive	hive-it-qfile-kudu	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-test-serde	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-unit	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-unit-hadoop2	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-it-util	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-jdbc	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-jdbc-handler	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-jmh	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-kryo-registrator	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-kudu-handler	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-llap-client	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-llap-common	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-llap-ext-client	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-llap-server	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-llap-tez	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-metastore	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-parser	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-pre-upgrade	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-serde	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-service	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-service-rpc	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-shims	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-spark-client	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-standalone-metastore	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-storage-api	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-streaming	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-testutils	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-udf	3.1.3000.7.2.11.0-233
	org.apache.hive	hive-vector-code-gen	3.1.3000.7.2.11.0-233
	org.apache.hive	kafka-handler	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-hcatalog-core	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-hcatalog-pig-adapter	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-hcatalog-server-extensions	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-hcatalog-streaming	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-webhcat	3.1.3000.7.2.11.0-233
	org.apache.hive.hcatalog	hive-webhcat-java-client	3.1.3000.7.2.11.0-233
	org.apache.hive.hive-udf-classloader-udf1 it-custom-udfs		3.1.3000.7.2.11.0-233
	org.apache.hive.hive-udf-classloader-udf2 it-custom-udfs		3.1.3000.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.hive.hive-it-custom-udfs	hive-udf-classloader-util	3.1.3000.7.2.11.0-233
	org.apache.hive.hive-it-custom-udfs	hive-udf-vectorized-badexample	3.1.3000.7.2.11.0-233
	org.apache.hive.shim	hive-shims-0.23	3.1.3000.7.2.11.0-233
	org.apache.hive.shim	hive-shims-common	3.1.3000.7.2.11.0-233
	org.apache.hive.shim	hive-shims-scheduler	3.1.3000.7.2.11.0-233
Apache Hive Warehouse Connector	com.hortonworks.hive	hive-warehouse-connector_2.11	1.0.0.7.2.11.0-233
Apache Kafka	org.apache.kafka	connect	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-api	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-basic-auth-extension	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-file	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-json	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-mirror	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-mirror-client	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-runtime	2.5.0.7.2.11.0-233
	org.apache.kafka	connect-transforms	2.5.0.7.2.11.0-233
	org.apache.kafka	generator	2.5.0.7.2.11.0-233
	org.apache.kafka	jmh-benchmarks	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-clients	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-cloudera-plugins	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-examples	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-log4j-appender	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-examples	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-scala_2.12	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-scala_2.13	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-test-utils	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-0100	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-0101	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-0102	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-0110	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-10	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-11	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-20	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-21	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-22	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-23	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka-streams-upgrade-system-tests-24	2.5.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.kafka	kafka-tools	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka_2.12	2.5.0.7.2.11.0-233
	org.apache.kafka	kafka_2.13	2.5.0.7.2.11.0-233
Apache Knox	org.apache.knox	gateway-adapter	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-admin-ui	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-applications	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-cloud-bindings	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-demo-ldap	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-demo-ldap-launcher	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-discovery-ambari	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-discovery-cm	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-docker	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-i18n	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-i18n-logging-log4j	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-i18n-logging-sl4j	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-performance-test	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-ha	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-common	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-concat	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-hadoop-groups	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-pseudo	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-regex	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-identity-assertion-switchcase	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-jersey	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-common	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-func-hostmap-static	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-func-inbound-query-param	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-func-service-registry	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-step-encrypt-uri	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-rewrite-step-secure-query	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-authc-anon	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-authz-acls	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-authz-composite	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-clientcert	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-hadoopauth	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-jwt	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-pac4j	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-preauth	1.3.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.knox	gateway-provider-security-shiro	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-provider-security-webappsec	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-release	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-server	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-server-launcher	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-server-xforwarded-filter	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-admin	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-as	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-definitions	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-hashicorp-vault	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-hbase	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-health	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-hive	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-idbroker	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-impala	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-jkg	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-knoxssso	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-knoxssout	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-knoxtoken	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-livy	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-metadata	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-nifi	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-nifi-registry	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-remoteconfig	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-rm	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-session	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-storm	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-test	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-tgs	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-vault	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-service-webhdfs	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-shell	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-shell-launcher	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-shell-release	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-shell-samples	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-spi	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-test	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-test-idbroker	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-test-release-utils	1.3.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.knox	gateway-test-utils	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-topology-hadoop-xml	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-topology-simple	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-util-common	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-util-configinjector	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-util-launcher	1.3.0.7.2.11.0-233
	org.apache.knox	gateway-util-urltemplate	1.3.0.7.2.11.0-233
	org.apache.knox	hadoop-examples	1.3.0.7.2.11.0-233
	org.apache.knox	knox-cli-launcher	1.3.0.7.2.11.0-233
	org.apache.knox	knox-homepage-ui	1.3.0.7.2.11.0-233
	org.apache.knox	webhdfs-kerb-test	1.3.0.7.2.11.0-233
	org.apache.knox	webhdfs-test	1.3.0.7.2.11.0-233
Apache Kudu	org.apache.kudu	kudu-backup-tools	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-backup2_2.11	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-backup3_2.12	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-client	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-hive	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-spark2-tools_2.11	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-spark2_2.11	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-spark3-tools_2.12	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-spark3_2.12	1.15.0.7.2.11.0-233
	org.apache.kudu	kudu-test-utils	1.15.0.7.2.11.0-233
Apache Livy	org.apache.livy	livy-api	0.6.0.7.2.11.0-233
	org.apache.livy	livy-client-common	0.6.0.7.2.11.0-233
	org.apache.livy	livy-client-http	0.6.0.7.2.11.0-233
	org.apache.livy	livy-core_2.11	0.6.0.7.2.11.0-233
	org.apache.livy	livy-examples	0.6.0.7.2.11.0-233
	org.apache.livy	livy-integration-test	0.6.0.7.2.11.0-233
	org.apache.livy	livy-repl_2.11	0.6.0.7.2.11.0-233
	org.apache.livy	livy-rsc	0.6.0.7.2.11.0-233
	org.apache.livy	livy-scala-api_2.11	0.6.0.7.2.11.0-233
	org.apache.livy	livy-server	0.6.0.7.2.11.0-233
	org.apache.livy	livy-test-lib	0.6.0.7.2.11.0-233
	org.apache.livy	livy-thriftserver	0.6.0.7.2.11.0-233
	org.apache.livy	livy-thriftserver-session	0.6.0.7.2.11.0-233
Apache Lucene	org.apache.lucene	lucene-analyzers-common	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-icu	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-kuromoji	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-morfologik	8.4.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.lucene	lucene-analyzers-nori	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-openslp	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-phonetic	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-smartcn	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-analyzers-stempel	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-backward-codecs	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-benchmark	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-classification	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-codecs	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-core	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-demo	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-expressions	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-facet	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-grouping	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-highlighter	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-join	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-memory	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-misc	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-monitor	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-queries	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-queryparser	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-replicator	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-sandbox	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-spatial	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-spatial-extras	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-spatial3d	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-suggest	8.4.1.7.2.11.0-233
	org.apache.lucene	lucene-test-framework	8.4.1.7.2.11.0-233
Apache Oozie	org.apache.oozie	oozie-client	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-core	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-distro	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-examples	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-fluent-job-api	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-fluent-job-client	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-server	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-distcp	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-git	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-hcatalog	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-hive	5.1.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.oozie	oozie-sharelib-hive2	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-oozie	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-spark	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-sqoop	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-sharelib-streaming	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-tools	5.1.0.7.2.11.0-233
	org.apache.oozie	oozie-zookeeper-security-tests	5.1.0.7.2.11.0-233
	org.apache.oozie.test	oozie-mini	5.1.0.7.2.11.0-233
Apache ORC	org.apache.orc	orc-core	1.5.1.7.2.11.0-233
	org.apache.orc	orc-examples	1.5.1.7.2.11.0-233
	org.apache.orc	orc-mapreduce	1.5.1.7.2.11.0-233
	org.apache.orc	orc-shims	1.5.1.7.2.11.0-233
	org.apache.orc	orc-tools	1.5.1.7.2.11.0-233
Apache Parquet	org.apache.parquet	parquet-avro	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-cascading	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-cascading3	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-column	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-common	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-encoding	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-format-structures	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-generator	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-hadoop	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-hadoop-bundle	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-jackson	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-pig	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-pig-bundle	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-protobuf	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-scala_2.10	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-thrift	1.10.99.7.2.11.0-233
	org.apache.parquet	parquet-tools	1.10.99.7.2.11.0-233
Apache Phoenix	org.apache.phoenix	phoenix-client-embedded-hbase-2.2	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-client-hbase-2.2	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-connectors-phoenix5-compatible	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-core	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-hbase-compatible-2.1.6	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-hbase-compatible-2.2.5	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-hbase-compatible-2.3.0	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-hbase-compatible-2.4.0	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-hbase-compatible-2.4.1	5.1.1.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.phoenix	phoenix-pherf	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-queryserver	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-queryserver-client	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-queryserver-it	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-queryserver-load-balancer	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-queryserver-orchestrator	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix-server-hbase-2.2	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-tools	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix-tracing-webapp	5.1.1.7.2.11.0-233
	org.apache.phoenix	phoenix5-hive	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix5-hive-shaded	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix5-spark	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix5-spark-shaded	6.0.0.7.2.11.0-233
	org.apache.phoenix	phoenix5-spark-shaded-commons-cli	1.1.0.7.2.11.0-233
	org.apache.phoenix	phoenix5-spark-shaded-guava	1.1.0.7.2.11.0-233
Apache Ranger	org.apache.ranger	conditions-enrichers	2.1.0.7.2.11.0-233
	org.apache.ranger	credentialbuilder	2.1.0.7.2.11.0-233
	org.apache.ranger	embeddedwebservice	2.1.0.7.2.11.0-233
	org.apache.ranger	jisql	2.1.0.7.2.11.0-233
	org.apache.ranger	ldapconfigcheck	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-adls-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-atlas-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-atlas-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-authn	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-distro	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-examples-distro	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hbase-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hbase-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hdfs-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hdfs-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hive-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-hive-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-intg	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kafka-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kafka-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kms	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kms-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kms-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-knox-plugin	2.1.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.ranger	ranger-knox-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kudu-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kylin-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-kylin-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-nifi-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-nifi-registry-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-ozone-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-ozone-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-plugin-classloader	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-plugins-audit	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-plugins-common	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-plugins-cred	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-plugins-installer	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-adls	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-hook-abfs	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-hook-s3	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-intg	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-processor	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-s3	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-raz-s3-lib	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-rms-common	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-rms-hive	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-rms-plugins-common	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-rms-webapp	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-s3-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-sampleapp-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-schema-registry-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-solr-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-solr-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-sqoop-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-sqoop-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-storm-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-storm-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-tagsync	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-tools	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-util	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-yarn-plugin	2.1.0.7.2.11.0-233
	org.apache.ranger	ranger-yarn-plugin-shim	2.1.0.7.2.11.0-233
	org.apache.ranger	sample-client	2.1.0.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.ranger	sampleapp	2.1.0.7.2.11.0-233
	org.apache.ranger	shaded-raz-hook-abfs	2.1.0.7.2.11.0-233
	org.apache.ranger	shaded-raz-hook-s3	2.1.0.7.2.11.0-233
	org.apache.ranger	ugsync-util	2.1.0.7.2.11.0-233
	org.apache.ranger	unixauthclient	2.1.0.7.2.11.0-233
	org.apache.ranger	unixauthservice	2.1.0.7.2.11.0-233
	org.apache.ranger	unixusersync	2.1.0.7.2.11.0-233
Apache Solr	org.apache.solr	solr-analysis-extras	8.4.1.7.2.11.0-233
	org.apache.solr	solr-analytics	8.4.1.7.2.11.0-233
	org.apache.solr	solr-cell	8.4.1.7.2.11.0-233
	org.apache.solr	solr-clustering	8.4.1.7.2.11.0-233
	org.apache.solr	solr-core	8.4.1.7.2.11.0-233
	org.apache.solr	solr-dataimporthandler	8.4.1.7.2.11.0-233
	org.apache.solr	solr-dataimporthandler-extras	8.4.1.7.2.11.0-233
	org.apache.solr	solr-jaegertracer-configurator	8.4.1.7.2.11.0-233
	org.apache.solr	solr-langid	8.4.1.7.2.11.0-233
	org.apache.solr	solr-ltr	8.4.1.7.2.11.0-233
	org.apache.solr	solr-prometheus-exporter	8.4.1.7.2.11.0-233
	org.apache.solr	solr-security-util	8.4.1.7.2.11.0-233
	org.apache.solr	solr-solrj	8.4.1.7.2.11.0-233
	org.apache.solr	solr-test-framework	8.4.1.7.2.11.0-233
	org.apache.solr	solr-velocity	8.4.1.7.2.11.0-233
Apache Spark	org.apache.spark	spark-avro_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-catalyst_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-core_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-graphx_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-hadoop-cloud_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-hive_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-kubernetes_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-kvstore_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-launcher_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-mllib-local_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-mllib_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-network-common_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-network-shuffle_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-network-yarn_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-repl_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-shaded-raz	2.4.7.7.2.11.0-233
	org.apache.spark	spark-sketch_2.11	2.4.7.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.spark	spark-sql-kafka-0-10_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-sql_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-streaming-kafka-0-10-assembly_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-streaming-kafka-0-10_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-streaming_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-tags_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-token-provider-kafka-0-10_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-unsafe_2.11	2.4.7.7.2.11.0-233
	org.apache.spark	spark-yarn_2.11	2.4.7.7.2.11.0-233
Apache Sqoop	org.apache.sqoop	sqoop	1.4.7.7.2.11.0-233
	org.apache.sqoop	sqoop-test	1.4.7.7.2.11.0-233
Apache Tez	org.apache.tez	hadoop-shim	0.9.1.7.2.11.0-233
	org.apache.tez	hadoop-shim-2.8	0.9.1.7.2.11.0-233
	org.apache.tez	tez-api	0.9.1.7.2.11.0-233
	org.apache.tez	tez-aux-services	0.9.1.7.2.11.0-233
	org.apache.tez	tez-common	0.9.1.7.2.11.0-233
	org.apache.tez	tez-dag	0.9.1.7.2.11.0-233
	org.apache.tez	tez-examples	0.9.1.7.2.11.0-233
	org.apache.tez	tez-ext-service-tests	0.9.1.7.2.11.0-233
	org.apache.tez	tez-history-parser	0.9.1.7.2.11.0-233
	org.apache.tez	tez-javadoc-tools	0.9.1.7.2.11.0-233
	org.apache.tez	tez-job-analyzer	0.9.1.7.2.11.0-233
	org.apache.tez	tez-mapreduce	0.9.1.7.2.11.0-233
	org.apache.tez	tez-protobuf-history-plugin	0.9.1.7.2.11.0-233
	org.apache.tez	tez-runtime-internals	0.9.1.7.2.11.0-233
	org.apache.tez	tez-runtime-library	0.9.1.7.2.11.0-233
	org.apache.tez	tez-tests	0.9.1.7.2.11.0-233
	org.apache.tez	tez-yarn-timeline-cache-plugin	0.9.1.7.2.11.0-233
	org.apache.tez	tez-yarn-timeline-history	0.9.1.7.2.11.0-233
	org.apache.tez	tez-yarn-timeline-history-with-acls	0.9.1.7.2.11.0-233
	org.apache.tez	tez-yarn-timeline-history-with-fs	0.9.1.7.2.11.0-233
Apache Zeppelin	org.apache.zeppelin	zeppelin-angular	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-display	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-interpreter	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-jdbc	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-jupyter	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-livy	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-markdown	0.8.2.7.2.11.0-233
	org.apache.zeppelin	zeppelin-server	0.8.2.7.2.11.0-233

Project	groupId	artifactId	version
	org.apache.zookeeper	zookeeper-shaded-raz	0.8.2.7.2.11.0-233
	org.apache.zookeeper	zookeeper-shell	0.8.2.7.2.11.0-233
	org.apache.zookeeper	zookeeper-zengine	0.8.2.7.2.11.0-233
Apache ZooKeeper	org.apache.zookeeper	zookeeper	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-client-c	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-contrib-loggraph	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-contrib-rest	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-contrib-zooinspector	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-docs	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-jute	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-recipes-election	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-recipes-lock	3.5.5.7.2.11.0-233
	org.apache.zookeeper	zookeeper-recipes-queue	3.5.5.7.2.11.0-233

What's New In Cloudera Runtime 7.2.11

You must be aware of the additional functionalities and improvements to features of components in Cloudera Runtime 7.2.11. Learn how the new features and improvements benefit you.

What's New in Apache HBase

Learn about the new features of Apache HBase in Cloudera Runtime 7.2.11.

--cldr.cross.domain option of the CldrCopyTable utility

CldrCopyTable is Cloudera's version of the upstream CopyTable utility. The new --cldr.cross.domain option of CldrCopyTable enables you to copy data cross-realm.

What's New in Apache Hive

There are no new features for Apache Hive in this release of Cloudera Runtime.

What's New in Apache Impala

Learn about the new features of Impala in Cloudera Runtime 7.2.11.

Added a new scale argument to the ndv() function

The optional argument scale must be an integer and can be in the range from 1 to 10 and maps to a precision used by the HyperLogLog (HLL) algorithm with the following mapping formula:

```
precision = scale + 8
```

See [NDV Function](#) for more information.

Added a new query option DELETE_STATS_IN_TRUNCATE

This query option DELETE_STATS_IN_TRUNCATE can be used to delete or retain table statistics. The default value of this option is 1 or true which means table statistics will be deleted as part of truncate operation.

See [Query Options](#) for more information.

Added a new query option KUDU_REPLICA_SELECTION

Using this new query option KUDU_REPLICA_SELECTION, the queries can be targeted to the leader-only replica and skip non-leader replicas while scanning. When the new query option KUDU_REPLICA_SELECTION is set as LEADER_ONLY, Impala planner will generate a query plan that enables Impala to scan Kudu tables at the leader-only replicas.

See [Query Options](#) for more information.

Added a new query option DEFAULT_NDV_SCALE

As a cluster admin, you can improve the precision of NDV() using this new query option DEFAULT_NDV_SCALE. You may adjust the value in this query option to change the default precision setting for NDV() so that the SQL writers do not have to rewrite the SQLs to adjust NDV's precision.

See [Query Options](#) for more information.

What's New in Apache Kafka

Learn about the new features of Apache Kafka in Cloudera Runtime 7.2.11.

New performance related health tests for Kafka

Two new health tests based on the kafka_request_handler_avg_idle_1min_rate and the kafka_network_processor_avg_idle metrics are added for Kafka in Cloudera Manager. The health tests added are the following the following:

- Request Handler Capacity

This health test checks the most recent value of the kafka_request_handler_avg_idle_1min_rate metric and sends a warning if less than 30% of request handler capacity is available. Additionally, the warning recommends that users increase the number of I/O threads using the Number of I/O Threads (num.io.threads) property.

- Network Processor Capacity

This health test checks the most recent value of the kafka_network_processor_avg_idle metric and sends a warning if less than 30% of network processor capacity is available. Additionally, the warning recommends that users increase the number of network threads using the Number of Network Threads (num.network.threads) property.

For more information, see [Cloudera Manager Health Tests Reference](#).

What's New in Apache Kudu

Learn about the new features of Apache Kudu in Cloudera Runtime 7.2.11.

Add --newDatabaseName and --removeImpalaPrefix options to restore job

While Kudu does not have the notion of a database, users typically define full table names as <database>.<tablename>. Two new options are added to enable you to change the existing database name of a restored table or add a new database name to a restored table. The --newDatabaseName option enables you to specify a new database name for the restored table. The --removeImpalaPrefix option removes the impala:: prefix if it exists. The --newDatabaseName option does not affect the impala:: prefix.

Per-table size and row count limits

Kudu now experimentally supports per-table size limits based on leader disk space usage or number of rows. When generating new authorization tokens, Masters will now consider the size limits and strip tokens of INSERT and UPDATE privileges if either limit is reached. To enable this feature, set the `--enable_table_write_limit` master flag; adjust the `--table_disk_size_limit` and `--table_row_count_limit` flags as desired or use the kudu table `set_limit` tool to set limits per table.

Improvements

- Backup graphs are sorted by table name to ensure the listing order stays consistent.
- KUDU-3267: The error message output by Kudu Java client in an attempt to write into a non-existent table partition now contains the table's name.

What's New in Apache Phoenix

Learn about the new features of Apache Phoenix in Cloudera Runtime 7.2.11.

Capturing DDL and DML statements

Previously only Select query logging was available in Phoenix. From now Phoenix supports the logging of DDL and DML queries as well.

What's New in Schema Registry

Learn about the new features of Schema Registry in Cloudera Runtime 7.2.11.

Schema Registry Confluent API needs a compatibility endpoint

A new endpoint that checks compatibility between schemas is now available to the Confluent-compatible API.

The endpoint is as follows:

```
/api/v1/confluent/compatibility/subjects/[***SCHEMA**]/version
s/[***VERSION***]
```

Where:

- `[***SCHEMA***]` is the name of the subject/schema.
- `[***VERSION***]` is the version that the new schema text is compared to. The version can be latest or a valid version ID.

When using the endpoint, you must specify the schema, version, and the schema text that you want to compare. The schema text can be sent as a data parameter. For example:

```
curl -X POST "http://\hostname\:9090/api/v1/confluent/compatibility/subjects/\schemaname/versions/latest" -H "accept: application/json" -H "Content-Type: application/json" -d "{\"schema\": \"{\\\"fields\\\": [{\\\"default\\\": \\\"yellow\\\", \\\"name\\\": \\\"color\\\", \\\"type\\\": [\\\"string\\\"]}], \\\"name\\\": \\\"schemaname\\\", \\\"type\\\": \\\"record\\\"}\"}
```

The endpoint responds with a compatibility result. This can either be true or false.

If the schema is compatible, the endpoint returns a true response. For example:

```
{ "compatible": true, "errorMessage": null, "errorLocation": null, "schema": "{\n  \"type\": \"record\",\n  \"name\": \"compatible\",\n  \"fields\": [\n    {\n      \"name\": \"compatible\",\n      \"type\": [\"string\"],\n      \"default\": \"test\"\n    }\n  ]\n}"}
```

If the schema is not compatible, the endpoint returns a false response. This response contains an error message as well as the location where the error was encountered. For example:

```
{ "compatible": false, "errorMessage": "reader union lacking writer type: STRING", "errorLocation": "/fields/0/type/0", "schema": "{ \"type\": \"record\", \"name\": \"compatible\", \"fields\": [{ \"name\": \"compatible\", \"type\": [\"string\"], \"default\": \"test\" } ] }" }
```

What's New in Cloudera Search

Learn about the new features of Cloudera Search in Cloudera Runtime 7.2.11.

Optimize phase of MRIT reducers can now be skipped

This release adds a new feature to MapReduceIndexerTool (MRIT) that allows skipping the optimize phase of reducers. To skip the optimize operation at the end of reducers set the value of the maxSegments parameter to 0 or -1.

What's New in Apache Spark

Learn about the new features of Spark in Cloudera Runtime 7.2.11.

Data engineering cluster

You can create a data engineering cluster in Amazon AWS from within CDP by selecting the Data Engineering cluster template. A data engineering includes Spark, Livy, Hive, Zeppelin, and Oozie, along with supporting services (HDFS, YARN, and Zookeeper).

See [Creating a Cluster on AWS](#).

What's New in Sqoop

Learn what's new in the Apache Sqoop client in Cloudera Runtime 7.2.11.

To access the latest Sqoop documentation on Cloudera's documentation web site, go to [Sqoop Documentation 1.4.7.1.6.0](#).

Discontinued maintenance of direct mode

The Sqoop direct mode feature is no longer maintained. This feature was primarily designed to import data from an abandoned database, which is no longer updated. Using direct mode has several drawbacks:

- Imports can cause an intermittent and overlapping input split.
- Imports can generate duplicate data.
- Many problems, such as intermittent failures, can occur.
- Additional configuration is required.

Do not use the --direct option in Sqoop import or export commands.

What's new in Streams Messaging Manager

Learn about the new features of Streams Messaging Manager in Cloudera Runtime 7.2.11.

The SMM API now hides email notifier SMTP passwords in its response

Previously the /notifiers endpoint returned the full configuration of the notifier. In the case of email notifiers, the configuration included the password of the SMTP server. API responses from now on do not include the password. As result of this change, the PASSWORD field of existing email notifiers is left blank when you edit them. If you decide to edit the notifier you must reenter the password.

What's New in Streams Replication Manager

Learn about the new features of Streams Replication Manager in Cloudera Runtime 7.2.11.

The SRM Service role tries to recover automatically if errors are encountered

The SRM Service role might encounter errors that make metrics processing impossible. An example of this is when the target Kafka cluster is not reachable. If such an error is encountered, the SRM Service role now tries to recover automatically. If recovery is successful, the SRM Service role continues to monitor replications and displays as healthy in Cloudera Manager. However, during recovery, until the recovery is successful, the role displays as unhealthy.

New health tests for the SRM Service role

New health tests are introduced for the SRM Service role. These health tests describe the state of the SRM Service role. If the SRM Service role encounters an error that makes metrics processing impossible, Cloudera Manager now correctly displays the SRM Service role as unhealthy.

The wait time before starting new connectors is now configurable

A new configuration property, connect.start.task.timeout.ms, is added. This property controls the timeout of the tasks executed when starting connectors. The default value of the property is 20000 ms. You can configure the property on a replication level through the Streams Replication Manager's Replication Configs Cloudera Manager property. For example:

```
[ ***ALIAS*** ]->[ ***ALIAS*** ].connect.start.task.timeout.ms=25000
```

Custom lists of supported/excluded cipher suites and TLS/SSL protocols are configurable for the SRM Service role

A number of new properties related to TLS/SSL are introduced for the SRM Service role. These properties allow users to customize which cipher suites and TLS/SSL protocols should be supported or excluded by the SRM Service role. The properties added are as follows:

- Supported SSL/TLS Cipher Suites
(streams.replication.manager.ssl.supportedCipherSuites)
- Excluded SSL/TLS Cipher Suites
(streams.replication.manager.ssl.excludedCipherSuites)
- Supported SSL/TLS Protocols
(streams.replication.manager.ssl.supportedProtocols)
- Excluded SSL/TLS Protocols
(streams.replication.manager.ssl.excludedProtocols)

What's New in Apache Hadoop YARN

Learn about the new features of Hadoop YARN in Cloudera Runtime 7.2.11.

Migrating database configuration to a new location

The operations performed on queues in Queue Manager UI are stored as Queue Manager versions. You can either store these versions in the default database location on the host or configure a new location using Cloudera Manager UI. For security reasons, if you do not want to allow users to access the default database, you can move the database file to an alternative location. During an upgrade, you can move the database file to some other location and then restore this file to the default location after the upgrade.

For more information, see [Migrating database configuration to a new location](#).

Queue Manager REST API

You can now use the Queue Manager REST APIs to automate the Queue Manager operations using the HTTP endpoints. The Queue Manager REST server exposes endpoints that provide the start, stop, add, delete, change queue capacity, and change queue properties operations.

For more information, see [Configuring and using Queue Manager REST API](#).

Read-only access to Yarn Queue Manager UI for non-admins



Note: Read-only access to Yarn Queue Manager UI is now a fully supported feature.

You can now allow non-admin users to access YARN Queue Manager in a read-only mode. You can either create a new user account with read-only role or use any existing user account with read-only role in Cloudera Manager to access YARN Queue Manager UI. In the read-only access mode, the user can view all the configurations but cannot make any changes to the configurations.

For more information, see [Provide read-only access to Queue Manager UI](#).

Fair sharing intra-queue preemption support



Note: Fair sharing intra-queue preemption is now a fully supported feature.

You can now enable intra-queue preemption for queues that are configured with fairness-based ordering. If the user has configured ordering-policies for queues (`yarn.scheduler.capacity.<queue-path>.ordering-policy`) to be Fair and if this new feature intra-queue preemption is enabled using YARN Queue Manager UI, then all the applications from the same user get a fair amount of resources. Thus, fair-ordering preemption now ensures that each application under a queue gets its fair-share, whether from a single user or several.

While that is for applications from a single user, for resource allocation across users, you can enforce a limit on each user's resource-usage by setting the user limits (`yarn.scheduler.capacity.<queue-path>.user-limit-factor`).

For more information about ordering policies, see [Set Ordering policies within a specific queue](#).

Lazy Preemption

You can now enable the LazyPreemption feature to optimize the selection of containers from queues for preemption. Containers are preempted only if the resources can be used by another application. The LazyPreemption feature makes resource preemption more efficient. It prevents excessive preemption and ensures that container selection is continuously optimized. LazyPreemption avoids scenarios when preempted resources cannot be used by the application that needs the resource, and then such preempted resources go back to the over-utilized queue again.

For more information, see [Enabling LazyPreemption](#).

Set default Partition Expression

You can set a default partition on a queue. The default partition is used if no partition is specified when the application is submitted to the queue. By default, this field is empty, so applications get containers from nodes without a partition or label.

For more information, see [Setting a default partition expression](#).

Dynamic Queue Scheduling (Tech Preview)

The Dynamic Queue Scheduling feature enables you to dynamically change queue resource allocation. Currently, the feature is only supported in relative resource allocation mode.

For more information, see [Dynamic Queue Scheduling](#).

Auto Queue Creation Template (Technical Preview)

You can set the minimum and maximum capacities using the Auto Queue Creation template. These capacities will be applied for every dynamic child queue under that particular parent queue.

For more information, see [Enable dynamic auto child creation in weight mode](#).

Dynamic Child Creation Improvements

- You can now enable dynamic child creation for all queues. Previously, there must be at least one static child queue under the parent queue for which you want to enable this feature.
- Auto queue creation depth limit - Auto queue creation depth limit limits the number of queue levels from a parent queue. While previously auto queue creation depth limit limited the levels of queue path relative to its first existing parent queue, now it limits the level of queue path relative to its first static parent queue.
- The Auto Queue Deletion feature - Dynamic queues are deleted automatically after 300 seconds of the last job finished on them. This feature is enabled by default but supported only in weight allocation mode. You can prevent the automatic deletion of dynamic queues by disabling the Auto Queue Deletion feature in Cloudera Manager. For more information, see [Disabling auto queue deletion](#).

Unaffected Components in this release

There are no new features for the following components in Cloudera Runtime 7.2.11: Apache Atlas – Data Analytics Studio – Apache HBase – Apache Hadoop HDFS – Apache Hive – Hue – Apache Knox – Apache Oozie – Apache Phoenix – Apache Ranger – Cloudera Search – Apache Solr – Streams Messaging Manager – Apache ZooKeeper

There are no new features for the following components in Cloudera Runtime 7.2.11:

- Apache Atlas
- Data Analytics Studio
- Apache HBase
- Apache Hadoop HDFS
- Apache Hive
- Apache Knox
- Apache Kudu
- Apache Oozie
- Apache Phoenix
- Apache Ranger
- Cloudera Search
- Apache Solr
- Streams Messaging Manager
- Apache ZooKeeper

Fixed Issues In Cloudera Runtime 7.2.11

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.

Fixed Issues in Atlas

Review the list of Apache Atlas issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26152: Handling of SET SERDE & SET FILEFORMAT for Create Table and CLUSTERED BY for Alter Table in Atlas

This issue is resolved.

Apache patch information

Apache patches in this release. These patches do not have an associated Cloudera bug ID.

- ATLAS-4269
- ATLAS-4064
- ATLAS-4106

Fixed Issues in Avro

There are no fixed issues for Avro in Cloudera Runtime 7.2.11.

Fixed Issues in Cloud Connectors

Review the list of Cloud Connectors issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-27264: HADOOP-17771. S3A Filesystem creation fails "Unable to find a region via the region provider chain."

This issue is resolved.

CDPD-26548: HADOOP-17338. Intermittent S3AInputStream failures: Premature end of Content-Length.

This issue is resolved.

CDPD-26441: S3A to add option fs.s3a.endpoint.region to set AWS region.

This introduces fs.s3a.endpoint.region, which can be used to set the region of the S3 bucket, and bypasses the parsing of the region from an endpoint.

CDPD-24982: HADOOP-17801. No error message printed in hadoop fs command line operations when S3 bucket does not exist.

This issue is resolved.

CDPD-24496: HADOOP-17511. Add an Audit plugin point for S3A auditing.

This issue is resolved.

CDPD-21205: HADOOP-13551. Collect AwsSdkMetrics in S3A FileSystem IOStatistics.

This issue is resolved.

CDPD-28880: Spark job fails with AccessDeniedException exception (s3-raz).

This issue is resolved.

CDPD-27678: Caching S3 signatures in Raz causes SignatureDoesNotMatch errors; leads tpccds queries run longer.

This issue is resolved.

CDPD-7510: Client side caching of Ranger AuthZ responses in case of ranged reads.

This issue is resolved.

Fixed issues in Cruise Control

There are no fixed issues for Cruise Control in Cloudera Runtime 7.2.11.

Fixed issues in Data Analytics Studio

There are no fixed issues for Data Analytics Studio in Cloudera Runtime 7.2.11.

Fixed Issues in Apache Hadoop

Review the list of Hadoop issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26975: HADOOP-17631. Configuration `${env.VAR:-FALLBACK}` should eval FALLBACK when `restrictSystemProps=true`.

This issue is resolved.

CDPD-5222: HADOOP-16660. ABFS: Make `RetryCount` in `ExponentialRetryPolicy` Configurable.

This issue is resolved.

HADOOP-17424: Replace `HTrace` with `No-Op` tracer. `HTrace` is not an active project and we no longer support it. Along with this change, the old, vulnerable `jackson-databind` dependency is dropped.

This issue is resolved.

HADOOP-11245: Update NFS gateway to use `Netty4`. The NFS gateway is rewritten using `netty4`.

This issue is resolved.

Apache Patch Information

- HADOOP-17631
- HADOOP-17424
- HADOOP-16660

Fixed Issues in HBase

Review the list of Apache HBase issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-28309: This change is trying to make the check of table existence backward compatible with `hbase-1.x` such that `CldrCopyTable` of `HBase-2.x` communicates with a `HBase-1.x` cluster.

Detail: in `checkOutputSpecs` when checking table existence with using connection to check with `hbase:meta`, it fails when we're communicating with different `hbase` versions, e.g. using `hbase-2.x` client checking with `hbase-1.x` cluster that a column `family` does not exist in `hbase-1.x`'s `hbase:meta`. This issue is resolved.

Apache Patch Information

- HBASE-25970 MOB data loss - incorrect concatenation of `MOB_FILE_REFS`
- HBASE-25929 `RegionServer` JVM crash when compaction
- HBASE-25665 Option to use hostname instead of canonical hostname for secure HBase cluster connection
- HBASE-24286 Automatically submit SCPs for unknown RS on startup

- HBASE-26124 Backport HBASE-25373 "Remove HTrace completely in code base and try to make use of OpenTelemetry"

Technical Service Bulletins

TSB 2021-506: Active HBase MOB files can be removed

For the latest update on this issue, see the corresponding Knowledge article: [TSB 2021-506: Active HBase MOB files can be removed](#)

Fixed Issues in HDFS

Review the list of HDFS issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-6100

This improvement makes HDFS NameNode leave safemode immediately if all blocks have reported in, reducing the cluster startup time.

OPSAPS-43909: Execution filter is not applied to Delete Policy.

Execution filter is now applied to Delete Policy also. This issue is now resolved.

Apache Patch Information

- HDFS-15632

Fixed Issues in Apache Hive

Review the list of Hive issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-22658: Refactored and optimized timestamp parsing

This issue is resolved.

CDPD-22411: This jira fixes the Jackson component usage by optimizing the usage with Jackson bom

This issue is resolved.

CDPD-21141: Hive build and packing removes shims-0.20 module which is no longer supported.

This issue is resolved.

CDPD-18307: Hive's pom file includes the internal version of spark to avoid CVEs

This issue is resolved.

CDPD-14639: This jira fixes CVE-2020-9488 by upgrading the log4j version to 2.13.2

This issue is resolved.

CDPD-5088: HMS/Ranger Spark view authorization plan.

This issue is resolved.

CDPD-1799: We disable the HiveServer2 webUI log type field, if the user doesn't have admin level privileges.

This issue is resolved.

CDPD-27050: Meta info "transactional_properties" was not getting set to "insert_only" in hive managed tables in ORC format even though it was provided in options explicitly while writing from spark application. It lead to table to be full ACID table instead of insert only transitional table.

This issue is resolved.

CDPD-25406: Change the default value for "spark.hiveAcid.parallel.partitioning.threshold" to 25.

This issue is resolved.

CDPD-26849: HWC: Data fetch query check fails after updates in HiveParser.

This issue is resolved.

Apache Patch Information

- HIVE-24768
- HIVE-8828
- HIVE-23560
- HIVE-24026
- HIVE-24500
- HIVE-24876

Fixed Issues in Hive Warehouse Connector

Review the list of Hive Warehouse Connector issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-27050: Meta info "transactional_properties" was not getting set to "insert_only" in hive managed tables in ORC format even though it was provided in options explicitly while writing from spark application. It lead to table to be full ACID table instead of insert only transitional table.

This issue is resolved.

CDPD-25406: Change the default value for "spark.hiveAcid.parallel.partitioning.threshold" to 25.

This issue is resolved.

CDPD-26849: HWC: Data fetch query check fails after updates in HiveParser.

This issue is resolved.

Fixed Issues in Hue

Review the list of Hue issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-25862: Remove hibernate dependency for Hue

Hue no longer depends on the hibernate-core JAR file.

CDPD-25569: Unable to submit Oozie job from S3 or ABFS File Browser, but works from HDFS File Browser

This issue is resolved.

CDPD-23847: Upgrade Spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421 and CVE-2018-15756

This issue is resolved.

Technical Service Bulletins

TSB-487: Cloudera Hue is vulnerable to Cross-Site Scripting attacks

For the latest update on this issue, see the corresponding Knowledge article: [TSB 2021-487: Cloudera Hue is vulnerable to Cross-Site Scripting attacks \(CVE-2021-29994, CVE-2021-32480, CVE-2021-32481\)](#)

Fixed Issues in Apache Impala

Review the list of Impala issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26295: This introduces the startup_filesystem_check_directories startup parameter which customizes Impalas permissions/access checks to look at a specific filesystem location

By default this checks the root of the default filesystem. This issue is resolved.

Apache Patch Information

- None

Fixed Issues in Apache Kafka

There are no fixed issues for Apache Kafka in Cloudera Runtime 7.2.11.

Fixed Issues in Apache Knox

Review the list of Knox issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26705: Removed trailing slashes service context generation in general while discovering services in Knox automatically. Additionally, to avoid regression, all UI and API_AND_UI type service definitions were modified to contain the trailing slash except the ones with query parameters.

This issue is resolved.

CDPD-26454: End-users can use the copy icon next to Target Base URL to copy the value to the clipboard.

This issue is resolved.

CDPD-26453: INFO level logging is available in Knoxs DB-based token management when the reaper thread removes expired tokens from the database.

This issue is resolved.

CDPD-26452: Caching the entire serialized JWT upon successful signature verification so that Knox wont try to re-verify the signature again in case the supplied JWT matches

This issue is resolved.

CDPD-26331: End-users are not allowed to enter comments longer than 255 characters

This issue is resolved.

CDPD-25826: From now on, Knox is able to store generated tokens in a relational database (only PostgreSQL is supported for now)

This issue is resolved.

CDPD-24603: Knox stores the generated passcode tokens securely in the configured relational database

This issue is resolved.

CDPD-23488: Fixed an issue where multiple sessions were created by Zeppelin UI when going via Knox

This issue is resolved.

CDPD-20209: Add SQL Stream Builder service definitions to Knox SQL Stream Builder Service definitions are added to Knox, which enables auto-discovery functionality via simplified topology management

This issue is resolved.

Apache patch information

Apache patches in this release. These patches do not have an associated Cloudera bug ID.

- KNOX-2623
- KNOX-2621
- KNOX-2617
- KNOX-2613
- KNOX-2603
- KNOX-2641
- KNOX-2581
- KNOX-2601

Fixed Issues in Apache Kudu

Review the list of Apache Kudu issues that are resolved in Cloudera Runtime 7.2.11.

KUDU-2181: Fix duplicate master address and remove unsafe flag tag

Kudu now supports Raft configuration change for Kudu masters and CLI tools for orchestrating addition and removal of masters in a Kudu cluster. These tools substantially simplify the process of migrating to multiple masters, recovering a dead master and removing masters from a Kudu cluster. For detailed steps, see the latest administration documentation. This feature is evolving and the steps to add, remove and recover masters may change in the future.

KUDU-3273: Fix NPE in AsyncKuduClient.discoverTablets() following the removal of a partition

A bug in the metacache of the Kudu Java client lead to a NullPointerException thrown. The bug manifested itself in situations when a range in a table was dropped after a client application had already opened the table.

KUDU-3277: Fix concurrent session flush issue in Java client

Fixed bug in Kudu Java client which manifested in AUTO_FLUSH_BACKGROUND sessions hung in a call to KuduSession.flush() method. Another sign of the bug were stuck data ingest workloads based on Java client (e.g., kudu-spark applications) with "java.lang.AssertionError: This Deferred was already called!" message in the logs.

Fixed Issues in Apache Oozie

Review the list of Oozie issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-27541: In case Yarn resource manager is in HA and the resource manager for an Oozie action was specified with an alias then Oozie failed to obtain the actual Yarn RM principal because it could not resolve the hostname for the alias. This did not cause an issue if there were no auth-to-local rules as Oozie did a fallback to use the short name from the principal template. For example it extracted "yarn" from "yarn/_HOST@ROOT.HWX.SITE". However when there are auth-to-local rules then Yarn could not map the short name. This was fixed by Oozie handling the case when Yarn is in HA and/or a resource manager address alias is used.

This issue is resolved.

CDPD-26692: The Oozie purge process for bundles is creating orphan coordinators. When purging bundle jobs and bundle actions, it does not always purge coordinator jobs, etc. This causes orphaned coordinators, meaning neither they nor their children will ever be purged due to the purge logic. Hence the purge logic was modified to only purge bundles and coordinators if all of their children (Workflows) can be purged.

This issue is resolved.

CDPD-25982: Fixing a regression introduced in CDPD-21870 where we fixed an issues where Oozie always used the unix user and not the Kerberos user. However this fix did not take the Kerberos name rules into consideration which is now fixed in scope of this ticket.

This issue is resolved.

OPSAPS-59215: Oozie fails to start with JNI Group Mapping in CDP.

Oozie will now use the Hadoop native libraries when JNI group mapping is enabled. This issue is resolved.

CDPD-28593: Oozie fails to start when Callback Servlet Authentication is turned on.

When the Callback authentication was enabled Oozie failed to start up. This issue is resolved.

Apache patch information

- OOZIE-3365
- OOZIE-3596

- OOOIE-3409

Fixed Issues in Phoenix

Review the list of Phoenix issues that are resolved in Cloudera Runtime 7.2.11.

Apache Patch Information

- PHOENIX-5215
- PHOENIX-6378
- PHOENIX-6456 Support query logging for DDL and DML
- PHOENIX-6378 Unbundle sqlline from phoenix-client-embedded, and use it in sqlline.py
- PHOENIX-6427 Create sequence fails in lowercase schema

Fixed Issues in Parquet

Review the list of Parquet issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-23436: Parquet dependency thrift has been updated to 0.14.1 to fix CVE-2020-13949.

This issue is resolved.

Apache Patch Information

- PARQUET-2005

Fixed Issues in Apache Ranger

Review the list of Ranger issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-27464: For ADLS service, the password field has type "string"; changed this type to "password";

This issue is resolved.

CDPD-27217: Created default policy for hbase user for hdfs component, which will be used while DataLack backup and restore.

This issue is resolved.

CDPD-26934: Fixed Htrace dependency.

This issue is resolved.

CDPD-26324: After this fix, deny access audits will contain policy Id/Version

This issue is resolved.

CDPD-26181: Fixes the issue of wrong jetty-client version used in Ranger. Correct jetty-client version is defined in cdpd_jetty_version in CDP build is used now.

This issue is resolved.

CDPD-25876: Updating user source when same user exists as an internal & later added from external source

This issue is resolved.

CDPD-25609: Added default basic audit filters for yarn, kudu, s3, nifi, nifi-registry, schema-registry components

This issue is resolved.

CDPD-25372: Removed unused .htaccess file.

This issue is resolved.

Apache Patch Information

- RANGER-3367
- RANGER-3347
- RANGER-3329
- RANGER-3297
- RANGER-3283
- RANGER-3261

Fixed Issues in Schema Registry

Review the list of Schema Registry issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26382: Schema Registry Client does not clear resources for daemon thread for Kerberos Login

Closing SchemaRegistryClient did not stop the threads managing KerberosLogin, so an application could end up with multiple open threads. This has been fixed and calling close() will also stop the Kerberos thread.

CDPD-25995: Fingerprint hashes are not consistent for Avro schemas

Previously, if there is a default null value in the schema text, the schema's fingerprint will be different with every restart of Schema Registry. With this fix, the default null values in the schema text will remain the same null values independent of restarting the Schema Registry service.

CDPD-25905: _orderByFields and name parameters on the API should not be mandatory

In the previous release, the "name" field was mandatory in the /search/schemas API endpoint. The intent was to make the API better, because searching without a "name" parameter returns an incorrect result. However, this was interpreted as a breaking change in the API and had to be reverted to maintain backward compatibility. Now it is again possible to send requests without providing a "name" parameter, and again this will return an incorrect result.

CDPD-25614: Clearing the cache throws a NPE

Fixed issue where invoking schemaRegistryClient.deleteSchema() caused a NullPointerException.

CDPD-21913: Rename properties in Schema Registry yaml file, remove the dots

Schema Registry uses the Dropwizard framework which allows overriding configuration properties from the command line. Due to implementation specifics, until now some of the properties could not be overridden. This issue is now resolved.

Schema Registry's StorageManager's init method's properties parameter has type StorageProviderConfiguration.

In Schema Registry's configuration file, StorageProviderConfiguration properties can be:

- DbType
- queryTimeoutInSecs

Properties that can be dataSourceClassName, dataSourceUrl, dataSourceUser, dataSourcePassword and connectionProperties can be:

- oracleNetSslVersion
- oracleNetSslServerDnMatch
- trustStore
- trustStoreType
- keyStore
- keyStoreType

CDPD-21617: Migrate lettuce to lettuce-io in cache module

The following classes have been removed from the cache module:

- CacheServiceRegistry
- CacheServiceLocalRegistry
- RedisCacheServiceBuilder
- RedisCacheService
- DataStoreBackedCacheService
- CacheServiceJsonFactory
- CacheServiceId
- CacheService
- CacheWriterSync
- CacheWriterAsync
- CacheWriter
- CacheLoaderSyncFactory
- CacheLoaderSync
- CacheLoaderFactory
- CacheLoaderCallback
- CacheLoaderAsyncFactory
- CacheLoaderAsync
- CacheLoader
- RedisConnectionPoolFactory
- RedisConnectionFactory
- AbstractRedisConnectionFactory
- RedisStringsCache
- RedisHashesCache
- RedisAbstractCache
- GuavaCache
- PhoenixDataStore
- DataStoreWriter
- DataStoreReader
- AbstractDataStore
- ViewConfig
- TypeConfig
- DataStoreConfig
- ConnectionConfig
- CachesConfig
- CacheEntry
- CacheConfig
- StaticFactory
- Factory
- DataStoreBackedCache
- CacheException
- LoadableCache
- AbstractCache

CDPD-17358: Add logging to Ranger filtering operations in Schema Registry

Logging added to show which schemas have been filtered out.

OPSAPS-59993: Disable admin port in Schema Registry

The following admin ports are no longer enabled in Schema Registry:

- Port 7791 on a secure cluster.
- Port 7789 on a unsecured cluster.

OPSAPS-59972: Disable the TRACE method on all HTTP ports

In Streams Messaging Manager and Schema Registry, the allowed HTTP methods are changed to GET, POST, PUT, DELETE, HEAD, OPTIONS.

OPSAPS-60458: Knox principal is not over-ridable in SMM and Schema Registry

Custom Knox principal can be set for Schema Registry and SMM by setting the `knox_principal_name` property in Schema Registry Server Advanced Configuration Snippet (Safety Valve) for `registry.yaml` or Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for `streams-messaging-manager.yaml`.

Fixed Issues in Apache Solr

There are no fixed issues for Apache Solr in Cloudera Runtime 7.2.11.

Fixed Issues in Spark

Review the list of Spark issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-27961: Insert overwrite no longer fails due to partition directory double delete

This issue is resolved.

Apache patch information

Apache patches in this release. These patches do not have an associated Cloudera bug ID.

- SPARK-17875
- SPARK-33841

Fixed Issues in Apache Sqoop

Review the list of Sqoop issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-25689: Fixing regression introduced in SQOOP-2846 when using update-key in Sqoop export command.

The problem occurred when Sqoop export was used with --update-key and --columns arguments at the same time. In this scenario, the --columns argument got ignored which is now fixed. This issue is resolved.

OPSAPS-59091: FUpgrading from CDH->CDP sets --parquet-configurator-implementation to unsupported option Kite, which breaks all Sqoop commands.

When upgrading to CDP 7.x Cloudera Manager will set the "parquetjob.configurator.implementation" configuration to "hadoop" for Sqoop as that's the only value supported. This issue is resolved.

Apache patch information

No additional Apache patches.

Fixed Issues in Streams Messaging Manager

Review the list of Streams Messaging Manager issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-26633: SMM API exposes email notifier SMTP password

The SMM API no longer returns the SMTP password in its responses to avoid sensitive information leak. This leaves the SMTP password field blank in the SMM UI when editing an email notifier provider. The password needs to be re-entered when any changes are made to its configurations.

Fixed Issues in Streams Replication Manager

Review the list of Streams Replication Manager issues that are resolved in Cloudera Runtime 7.2.11.

CDPD-13864 and CDPD-15327: Replication stops after the network configuration of a source or target cluster is changed

This issue is fixed.

OPSAPS-60601: The SRM client's secure storage might become corrupted if the JAAS Secret properties are used

JAAS secrets can be used in Kafka External Accounts.

OPSAPS-60601: Replication does not start when the target cluster of the replication is unsecured

Unsecure clusters can now be targeted by replications.

OPSAPS-60775: Kafka External Accounts configurations are not generated for the SRM Service

The SRM Service's configuration now contains the Kafka External Accounts configuration, enabling SRM Service to access Kafka clusters defined through External Accounts.

Fixed Issues in Apache Hadoop YARN

Review the list of Hadoop YARN issues that are resolved in Cloudera Runtime 7.2.11.

COMPX-7072: Backport YARN-8721 to fix node attribute issues when node is removed and then added back with same hostname.

This issue is resolved.

COMPX-7051: When YARN Nodemanagers are downscaled and then upscaled reusing the same hostnames, YARN will stop scheduling containers on these NodeManagers unless ResourceManager is restarted

This issue is resolved.

COMPX-6447: RM HA initial startup can randomly fail due to race conditions in ZKConfigurationStore

This issue is resolved.

COMPX-6143: CB changes is picked up and now adds Node Attributes config to YARN from the template

This issue is resolved.

COMPX-5689: Fix queue sort options in weight mode

This issue is resolved.

COMPX-5256: Allow to create empty dynamic auto creation enabled parent queue

Previously you had to create at least one static queue under the queue for which you wanted to enable the dynamic auto queue creation feature. It is no longer required, the feature can be enabled for a queue without any child queue as well.

COMPX-4890: Unable to delete a queue after unassigning a node label

When user tries to delete a queue a warning message displayed to indicate that queue can not be deleted without re-allocating the node-label capacity of the queue to be deleted.

Apache patch information

- YARN-8721
- YARN-10807
- YARN-10869

Fixed Issues in Zeppelin

Review the list of Zeppelin issues that are resolved in Cloudera Runtime 7.2.11.

- CDPD-24981: Zeppelin notebook can not create table with jdbc phoenix interpreter
- CDPD-23410: Zeppelin notebook_authorizations::test_only_owners_can_change_permissions test is failing
- CDPD-22469: ZEPPELIN-5231: Livy Interpreter doesn't support Japanese Character - Encoding Issue
- CDPD-17187: Zeppelin - Upgrade to Angular 1.8.0 due to CVEs
- CDPD-20908: Remove log4j-slf4j-impl from JDBC/Hive interpreter
- CDPD-19308: Zeppelin - Upgrade to slf4j 1.7.30
- CDPD-19316: Zeppelin - Upgrade httpClient to 4.5.13+ / 5.0.3+ due to CVE-2020-13956
- CDPD-20461: Zeppelin - Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- CDPD-20267: Zeppelin build failure on cdpd-master
- CDPD-17471: [ZEPPELIN-5116]Accessing zeppelin via Knox after Knox logout should be redirected to Knox login page
- CDPD-17933: Zeppelin - Upgrade Spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- CDPD-19243: Upgrade to Shiro 1.7.0 due to CVE-2020-17510
- CDPD-18170: Zeppelin - Upgrade or remove auto-value due to shaded Guava CVEs

- CDPD-15497: Harmonize joda-time to version 2.10.6(cdpd harmonized)
- CDPD-17543: Zeppelin UI is not compiling due to Corrupted notebooks
- CDPD-16197: Upgrade api-*-1.0.0.jar due to CVEs
- CDPD-16096: Zeppelin - upgrade google-oauth-client to 1.31.0
- CDPD-17017: Upgrade xercesImpl to to 2.12.0 due to CVE-2018-2799
- CDPD-16845: Upgrade to Shiro 1.6.0 (CVE-2020-13933)
- CDPD-16111: Upgrade jsoup-1.7.2 (CVE-2015-6748)
- CDPD-16104: Upgrade postgresql JDBC driver to 42.2.16
- CDPD-14569: [ZEPPELIN-4414]. Upgrade thrift to 0.13
- CDPD-13378: Bumup version of Java Native Access (JNA)
- CDPD-16114 Upgrade jackrabbit-webdav 1.5.2 due to CVE-2015-1833
- CDPD-16115: Upgrade jgit due to CVE-2016-5725
- CDPD-14614: Update Spring Framework for Zeppelin (CVE-2018-1270)
- CDPD-11599: Update Quartz Enterprise Job Scheduler for Zeppelin (CVE-2019-13990)
- CDPD-14580: Upgrade Scala for CVEs
- BUG-124121: Password hashing not working in Zeppelin
- CDPD-15628: Compilation failure on dex-box
- CDPD-12920: Upgrade nimbus-jose-jwt to 7.9
- CDPD-14990: Upgrade libpam4j to 1.11 (CVE-2017-12197)
- CDPD-11426: Ensure consistent usage of jackson to 2.10.3
- CDPD-14579: remove org.reflections (CVE-2020-10683)
- CDPD-14581: Update Spring Framework for Zeppelin in 7.2.1.0 (CVE-2018-1275)
- CDPD-14369: [ZEPPELIN-4736] The use of SslContextFactory is deprecated
- CDPD-11406: Include NOTICE and LICENSE files in component directories
- CDPD-11301: Remove jackson and jersey-bundle
- CDPD-11780: Zeppelin: Remove spark (and other interpreters that are not shipped) source dependencies
- CDPD-11348: Update log4j to address CVE-2019-17571
- CDPD-11501: Update Apache Shiro for Zeppelin to 1.5.3
- CDPD-11571: Zeppelin build failure on cdpd-master due to perfect-scrollbar
- CDPD-10187: Zeppelin - Incorrect version of jackson-mapper-asl in CDP
- CDPD-9119: Zeppelin - Upgrade to Guava 28.1 to avoid CVE-2018-1023
- CDPD-9030: Upgrade jackson-databind to version 2.9.10.3 [CVE-2020-8840]
- CDPD-9454: [ZEPPELIN-4697] Zeppelin scheduler pings terracotta.org
- CDPD-8163: Remove `org.spark-project.hive` dependency
- CDPD-7789: Zeppelin - Upgrade to Jetty 9.4.26 to avoid CVEs
- CDPD-7479: add hadoop-cloud-storage jar in Zeppelin
- CDPD-3600: Sync Zeppelin with community latest version (0.8.2)
- CDPD-2933: [ZEPPELIN-4272] Zeppelin fails to use s3a configured for zeppelin.notebook.dir
- CDPD-1683: KerberosRealm roles should match with local file system, if nothing is specified
- CDPD-2300: Initialize proxyuser with proper configuration
- CDPD-1491: Zeppelin should support doAs
- BUG-120595: [ZEPPELIN-4197] Upgrade Jackson to 2.9.9
- BUG-120606: [ZEPPELIN-4187] Bump up version of Scala from 2.11.8 to 2.11.12 (#3378)
- BUG-120605: [ZEPPELIN-4186] Bump up version of org.jsoup:jsoup (#3377)
- BUG-120596: [ZEPPELIN-4188] Upgrade Jetty to 9.4.18.v20190429
- BUG-120594: ZEPPELIN-4193 Upgrade Bouncy Castle bcpkix-jdk15on to 1.60
- BUG-120593: [ZEPPELIN-4185] Upgrade Thrift to 0.12.0 (#3376)
- CDPD-1009: ZEPPELIN-4168: Use secure URLs for Maven repositories (#3370)
- CDPD-717: [Zeppelin 3792] Zeppelin SPNEGO support
- BUG-109581: [ZEPPELIN-3741] Do not clear "Authorization" header if Z-server is running behind proxy

- BUG-106906: Add shiro-tools-hasher in Zeppelin
- BUG-106297: JDBC interpreter log file is missing in zeppelin log directory
- BUG-102172: Include Google Connector in Zeppelin
- BUG-98604: Correct tutorial link should be added in interpreter page
- BUG-100845: Remove livy2.pyspark3 interpreter on zeppelin side
- BUG-114354: Fixes to make s3 storage work
- BUG-114354: Change Zeppelin to use unshaded jars
- BUG-103954: Exclude other dependencies in STS shaded JDBC driver to prevent conflict
- BUG-103715: fix handshake_failure download
- CDPD-10288: Zeppelin Notebook Initialisation fails with CNF error in RAZ Enabled Cluster

Apache Patch Information

- ZEP-79: Disable fs.file.impl cache to ensure RawLocalFS is used
- ZEP-97: [ZEPPELIN-3690] display all column with the same name in ui-grid

Fixed Issues in Apache ZooKeeper

There are no fixed issues for ZooKeeper in Cloudera Runtime 7.2.11.

Fixed Issues In Cloudera Runtime 7.2.11.9

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.9.

The following issues are resolved:

- HOTREQ-950 IDBroker client excessively adds SSL client config causing OOM issues
- HOTREQ-964 Release: HIVE-25574: Replace clob with varchar when storing creation metadata
- HOTREQ-917 HotFix Request for TSB 2022-543 for Public Cloud 7.2.12 Azure Environment

Fixed Issues In Cloudera Runtime 7.2.11.10

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.10.

The following issues are resolved:

- HOTREQ-1091 - ITAU Casting invalid dates does not produce NULL
- HOTREQ-1114 - Hue does not work with medium duty DL because IDBroker configuration has comma separated URLs
- HOTREQ-1036 - Bug Fix for SPARK-39083

Fixed Issues In Cloudera Runtime 7.2.11.11

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.11.

The following issues are resolved:

- HOTREQ-1178 - CDPD-44832 - HUE Oozie workflow rerun fails.

Fixed Issues In Cloudera Runtime 7.2.11.12

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.12.

The following issue is resolved:

- HOTREQ-1201 - HADOOP-18476 - ABFS and S3A FileContext bindings to close wrapped filesystems in finalizer

Fixed Issues In Cloudera Runtime 7.2.11.13

You can review the list of reported issues and their fixes in Cloudera Runtime 7.2.11.13.

The following issue is resolved:

- HOTREQ-1321 - Hotfix for CVE-2022-25168 in CDP 7.2.11 version.

Service Pack in Cloudera Runtime 7.2.11

You can review the list of CDP Public Cloud hotfixes rolled into Cloudera Runtime 7.2.11. This will help you to verify if a hotfix provided to you on a previous CDP Public Cloud release was included in this release.

- HOTFIX-5074

Known Issues In Cloudera Runtime 7.2.11

You must be aware of the known issues and limitations, the areas of impact, and workaround in Cloudera Runtime 7.2.11.

Known Issues in Apache Atlas

Learn about the known issues in Apache Atlas, the impact or changes to the functionality, and the workaround.

OPSAPS-61656: Service monitor leaking Truststore reloader threads.

Go to the atlas configuration and set atlas_server_url_canary_enabled to false.

CDPD-24089: Atlas creates HDFS path entities for GCP path and the qualified name of those entities does not have a cluster name appended.

None

CDPD-22082: ADLS Gen2 metadata extraction: If the queue is not cleared before performing Incremental extraction, messages are lost.

After successfully running Bulk extraction, you must clear the queue before running Incremental extraction.

CDPD-19996: Atlas AWS S3 metadata extractor fails when High Availability is configured for IDBroker.

If you have HA configured for IDBroker, make sure your cluster has only one IDBroker address in core-site.xml. If your cluster has two IDBroker addresses in core-site.xml, remove one of them, and the extractor must be able to retrieve the token from IDBroker.

CDPD-19798: Atlas /v2/search/basic API does not retrieve results when the search text mentioned in the entity filter criteria (like searching by Database or table name) has special characters like + - & ! () { } [] ^ " ~ * ? :

You can invoke the API and mention the search string (with special characters) in the query attribute in the search parameters.

ATLAS-3921: Currently there is no migration path from AWS S3 version 1 to AWS S3 version 2.

None

CDPD-12668: Navigator Spark lineage can fail to render in Atlas

As part of content conversion from Navigator to Atlas, the conversion of some spark applications created a cyclic lineage reference in Atlas, which the Atlas UI fails to render. The cases occur when a Spark application uses data from a table and updates the same table.

None

CDPD-11941: Table creation events missed when multiple tables are created in the same Hive command

When multiple Hive tables are created in the same database in a single command, the Atlas audit log for the database may not capture all the table creation events. When there is a delay between creation commands, audits are created as expected.

None

CDPD-11940: Database audit record misses table delete

When a hive_table entity is created, the Atlas audit list for the parent database includes an update audit. However, at this time, the database does not show an audit when the table is deleted.

None

CDPD-11790: Simultaneous events on the Kafka topic queue can produce duplicate Atlas entities

In normal operation, Atlas receives metadata to create entities from multiple services on the same or separate Kafka topics. In some instances, such as for Spark jobs, metadata to create a table entity in Atlas is triggered from two separate messages: one for the Spark operation and a second for the table metadata from HMS. If the process metadata arrives before the table metadata, Atlas creates a temporary entity for any tables that are not already in Atlas and reconciles the temporary entity with the HMS metadata when the table metadata arrives.

However, in some cases such as when Spark SQL queries with the write.saveAsTable function, Atlas does not reconcile the temporary and final table metadata, resulting in two entities with the same qualified name and no lineage linking the table to the process entity.

This issue is not seen for other lineage queries from spark:

```
create table default.xx3 as select * from default.xx2
insert into yy2 select * from yy
insert overwrite table ww2 select * from ww1
```

Another case where this behavior may occur is when many REST API requests are sent at the same time.

None

CDPD-11692: Navigator table creation time not converted to Atlas

In converting content from Navigator to Atlas, the create time for Hive tables is not moved to Atlas.

None

CDPD-11338: Cluster names with upper case letters may appear in lower case in some process names

Atlas records the cluster name as lower case in qualifiedNames for some process names. The result is that the cluster name may appear in lower case for some processes (insert overwrite table) while it appears in upper case for other queries (ctas) performed on the same cluster.

None

CDPD-10576: Deleted Business Metadata attributes appear in Search Suggestions

Atlas search suggestions continue to show Business Metadata attributes even if the attributes have been deleted.

None

CDPD-10574: Suggestion order doesn't match search weights

At this time, the order of search suggestions does not honor the search weight for attributes.

None

CDPD-9095: Duplicate audits for renaming Hive tables

Renaming a Hive table results in duplicate ENTITY_UPDATE events in the corresponding Atlas entity audits, both for the table and for its columns.

None

CDPD-7982: HBase bridge stops at HBase table with deleted column family

Bridge importing metadata from HBase fails when it encounters an HBase table for which a column family was previously dropped. The error indicates:

```
Metadata service API org.apache.atlas.AtlasClientV2$API_V2@58112bc4 failed with status 404 (Not Found) Response Body
({ "errorCode": "ATLAS-404-00-007", "errorMessage": "Invalid instance creation/updation parameters passed : hbase_column_family.table: mandatory attribute value missing in type hbase_column_family" })
```

None

CDPD-7781: TLS certificates not validated on Firefox

Atlas is not checking for valid TLS certificates when the UI is opened in FireFox browsers.

None

CDPD-6675: Irregular qualifiedName format for Azure storage

The qualifiedName for hdfs_path entities created from Azure blob locations (ABFS) doesn't have the clusterName appended to it as do hdfs_path entities in other location types.

None

CDPD-5933 and CDPD-5931: Unexpected Search Results When Using Regular Expressions in Basic Searches on Classifications

When you include a regular expression or wildcard in the search criteria for a classification in the Basic Search, the results may differ unexpectedly from when full classification names are included. For example, the Exclude sub-classifications option is respected when using a full classification name as the search criteria; when using part of the classification name and the wildcard (*) with Exclude sub-classifications turned off, entities marked with sub-classifications are not included in the results. Other instances of unexpected results include case-sensitivity.

None

CDPD-4762: Spark metadata order may affect lineage

Atlas may record unexpected lineage relationships when metadata collection from the Spark Atlas Connector occurs out of sequence from metadata collection from HMS. For example, if an ALTER TABLE operation in Spark changing a table name and is reported to Atlas before HMS has processed the change, Atlas may not show the correct lineage relationships to the altered table.

None

CDPD-4545: Searches for Qualified Names with "@" doesn't fetch the correct results

When searching Atlas qualifiedName values that include an "@" character (@), Atlas does not return the expected results or generate appropriate search suggestions.

Consider leaving out the portion of the search string that includes the @ sign, using the wildcard character * instead.

CDPD-3208: Table alias values are not found in search

When table names are changed, Atlas keeps the old name of the table in a list of aliases. These values are not included in the search index in this release, so after a table name is changed, searching on the old table name will not return the entity for the table.

None

CDPD-3160: Hive lineage missing for INSERT OVERWRITE queries

Lineage is not generated for Hive INSERT OVERWRITE queries on partitioned tables. Lineage is generated as expected for CTAS queries from partitioned tables.

None

CDPD-3125: Logging out of Atlas does not manage the external authentication

At this time, Atlas does not communicate a log-out event with the external authentication management, Apache Knox. When you log out of Atlas, you can still open the instance of Atlas from the same web browser without re-authentication.

To prevent access to Atlas after logging out, close all browser windows and exit the browser.

CDPD-1892: Ranking of top results in free-text search not intuitive

The Free-text search feature ranks results based on which attributes match the search criteria. The attribute ranking is evolving and therefore the choice of top results may not be intuitive in this release.

If you don't find what you need in the top 5 results, use the full results or refine the search.

CDPD-1884: Free text search in Atlas is case sensitive

The free text search bar in the top of the screen allows you to search across entity types and through all text attributes for all entities. The search shows the top 5 results that match the search terms at any place in the text (*term* logic). It also shows suggestions that match the search terms that begin with the term (term* logic). However, in this release, the search results are case-sensitive.

If you don't see the results you expect, repeat the search changing the case of the search terms.

CDPD-1823: Queries with ? wildcard return unexpected results

DSL queries in Advanced Search return incorrect results when the query text includes a question mark (?) wildcard character. This problem occurs in environments where trusted proxy for Knox is enabled, which is always the case for CDP.

None

CDPD-1664: Guest users are redirected incorrectly

Authenticated users logging in to Atlas are redirected to the CDP Knox-based login page. However, if a guest user (without Atlas privileges) attempts to log in to Atlas, the user is redirected instead to the Atlas login page.

To avoid this problem, open the Atlas Dashboard in a private or incognito browser window.

CDPD-922: IsUnique relationship attribute not honored

The Atlas model includes the ability to ensure that an attribute can be set to a specific value in only one relationship entity across the cluster metadata. For example, if you wanted to add metadata tags to relationships that you wanted to make sure were unique in the system, you could design the relationship attribute with the property "IsUnique" equal true. However, in this release, the IsUnique attribute is not enforced.

None

CDPD-24058: The Atlas-Kafka hook creates a new entity instead of linking them

When the `import-kafka.sh` tool is used and later the plugin is enabled in Kafka configurations, new incomplete topic entities is created. The tool is not linking the existing topics with the clients.

None

Known Issues in Apache Avro

This topic describes known issues and workarounds for using Avro in this release of Cloudera Runtime.

CDPD-23451: Remove/replace jackson-mapper-asl dependency.

Avro library depends on the already EOL `jackson-mapper-asl 1.9.13-cloudera.1` that also contains a couple of CVEs. The jackson library is part of the Avro API so cannot be changed without a complete rebase.

None.

Known Issues in Data Analytics Studio

Learn about the known issues in Data Analytics Studio, the impact or changes to the functionality, and the workaround.

- You may not be able to add or delete columns or change the table schema after creating a new table using the upload table feature.
- For clusters secured using Knox, you see the HTTP 401: Forbidden error message when you click the DAS quick link from Cloudera Manager and are unable to log into DAS.

Workaround: The admin user will need to provide the DAS URL from the Knox proxy topology to the users needing access to DAS.

- The download logs feature may not return the YARN application logs on a Kerberized cluster. When you download the logs, the logs contain an `error-reports.json` file which states that no valid Kerberos tokens are available.

Workaround: An admin user with access to the machine can use the `kinit` command as a hive user with hive service user keytabs and trigger the download.

- The task logs for a particular task may not be available in the task swimlane. And the zip file generated by download logs artifact may not have task logs, but instead contain an `error-reports.json` file with the error log of the download failures.
- You may not see any data for a report for any new queries that you run. This can happen especially for the last one day's report.

Workaround:

1. Shut down the DAS Event Processor.
2. Run the following command from the Postgres server:

```
update das.report_scheduler_run_audit set status = 'FAILED' where status = 'READING' ;
```

3. Start the DAS Event Processor.
- On clusters secured with Knox proxy only: You might not be able to save the changes to the JDBC URL in the DAS UI to change the server interface (HS2 or LLAP) on which you are running your queries.
 - You may be unable to upload tables or get an error while browsing files to upload tables in DAS on a cluster secured using Knox proxy.

- DAS does not parse semicolons (;) and double hyphens (--) in strings and comments.

For example, if you have a semicolon in query such as the following, the query might fail: `select * from properties where prop_value = "name1;name2";`

If a semicolon is present in a comment, then run the query after removing the semicolon from the comment, or removing the comment altogether. For example:

```
select * from test; -- select * from test;
select * from test; /* comment; comment */
```

Queries with double hyphens (--) might also fail. For example:

```
select * from test where option = '--name';
```

- You might face UI issues on Google Chrome while using faceted search. We recommend you to use the latest version of Google Chrome (version 71.x or higher).
- Visual Explain for the same query shows different graphs on the **Compose** page and the **Query Details** page.
- While running some queries, if you restart HSI, the query execution is stopped. However, DAS does not reflect this change and the queries appear to be in the same state forever.
- After a fresh installation, when there is no data and you try to access the Reports tab, DAS displays an "HTTP 404 Not Found" error.
- Join count does not get updated for tables with partitioned columns.

Known Issues in Apache HBase

This topic describes known issues and workarounds for using HBase in this release of Cloudera Runtime.

OpDB Data Hub cluster fails to initialize if you are reusing a cloud storage location that was used by an older OpDB Data Hub cluster

Workaround: Stop HBase using Cloudera Manager before deleting an operational database Data Hub cluster.

IntegrationTestReplication fails if replication does not finish before the verify phase begins

During `IntegrationTestReplication`, if the verify phase starts before the replication phase finishes, the test will fail because the target cluster does not contain all of the data. If the HBase services in the target cluster does not have enough memory, long garbage-collection pauses might occur.

Workaround: Use the `-t` flag to set the timeout value before starting verification.

HDFS encryption with HBase

Cloudera has tested the performance impact of using HDFS encryption with HBase. The overall overhead of HDFS encryption on HBase performance is in the range of 3 to 4% for both read and update workloads. Scan performance has not been thoroughly tested.

Workaround: N/A

AccessController postOperation problems in asynchronous operations

When security and Access Control are enabled, the following problems occur:

- If a Delete Table fails for a reason other than missing permissions, the access rights are removed but the table may still exist and may be used again.
- If `hbaseAdmin.modifyTable()` is used to delete column families, the rights are not removed from the Access Control List (ACL) table. The `postOperation` is implemented only for `postDeleteColumn()`.
- If Create Table fails, full rights for that table persist for the user who attempted to create it. If another user later succeeds in creating the table, the user who made the failed attempt still has the full rights.

Workaround: N/A

Apache Issue: [HBASE-6992](#)

Bulk load is not supported when the source is the local HDFS

The bulk load feature (the `completebulkload` command) is not supported when the source is the local HDFS and the target is an object store, such as S3/ABFS.

Workaround: Use `distcp` to move the HFiles from HDFS to S3 and then run bulk load from S3 to S3.

Apache Issue: N/A

Technical Service Bulletins

TSB 2023-667: HBase snapshot export failure can lead to data loss

When using Replication Manager for Apache HBase (HBase) snapshot replication, data loss will occur if both of the following conditions are met: (i) the external account used for the operation has delete access to the target storage location, and (ii) the snapshot export fails. If these conditions are met, the cleanup operation, which is automatically performed after the failure, would delete all data in the root folder of the snapshot, not only the snapshot files. If the user account does not have the delete permission on the target folder, the data remains unaffected.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2023-667: HBase snapshot export failure can lead to data loss](#)

Known Issues in HDFS

Learn about the known issues in HDFS, the impact or changes to the functionality, and the workaround.

OPSAPS-55788: WebHDFS is always enabled. The Enable WebHDFS checkbox does not take effect.

None.

Unsupported Features

The following HDFS features are currently not supported in Cloudera Data Platform:

- ACLs for the NFS gateway ([HADOOP-11004](#))
- Aliyun Cloud Connector ([HADOOP-12756](#))
- Allow HDFS block replicas to be provided by an external storage system ([HDFS-9806](#))
- Consistent standby Serving reads ([HDFS-12943](#))
- Cost-Based RPC FairCallQueue ([HDFS-14403](#))
- HDFS Router Based Federation ([HDFS-10467](#))
- More than two NameNodes ([HDFS-6440](#))
- NameNode Federation ([HDFS-1052](#))
- NameNode Port-based Selective Encryption ([HDFS-13541](#))
- Non-Volatile Storage Class Memory (SCM) in HDFS Cache Directives ([HDFS-13762](#))
- OpenStack Swift ([HADOOP-8545](#))
- SFTP FileSystem ([HADOOP-5732](#))
- Storage policy satisfier ([HDFS-10285](#))

Technical Service Bulletins

TSB 2021-531: HDFS Namenode checkpoints not running after installing or upgrading to CDP 7.1.7 in a TLS enabled cluster

HDFS Namenode checkpoints will not run correctly after installing or upgrading to CDP 7.1.7 in a TLS enabled cluster. Recent CDP Public Cloud releases are also affected, see full list of affected CDP releases below.

In an HDFS cluster with High Availability, the Standby NameNode (SBN) is responsible for periodically generating a new checkpoint (also called an FsImage). The standby NameNode then uploads this checkpoint to the Active NameNode (ANN). The purpose of the checkpoint is to reduce the NameNode's startup time by reducing the number of edit logs that must be replayed on NameNode restart.

The image upload from the SBN to ANN is performed over the HTTP protocol using an embedded Jetty HTTP server in the ANN. Due to a bug in the Jetty version 9.4.39 shipped with CDP, this checkpoint upload can fail and the ANN will not receive new FsImage files. The following error is seen in the SBN service logs.

```
java.io.IOException: Exception during image upload
```

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-531: HDFS Namenode checkpoints not running after installing or upgrading to CDP 7.1.7 in a TLS enabled cluster](#)

TSB 2023-666: Out of order HDFS snapshot deletion may delete renamed/moved files, which may result in data loss

Cloudera has discovered a bug in the Apache Hadoop Distributed File System (HDFS) snapshot implementation. Deleting an HDFS snapshot may incorrectly remove files in the .Trash directories or remove renamed files from the current file system state. This is an unexpected behavior because deleting an HDFS snapshot should only delete the files stored in the specified snapshot, but not data in the current state.

In the particular HDFS installation in which the bug was discovered, deleting one of the snapshots caused certain files to be moved to trash and deletion of some of the files in a .Trash directory. Although it is clear that the conditions of the bug are (1) out-of-order snapshot deletion and (2) files moved to trash or other directories, we were unable to replicate the bug in other HDFS installations after executing similar test operations with a variety of different sequences. We also did not observe any actual data loss in our tests. However, there is a remote possibility that this bug may lead to data loss.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2023-666: Out of order HDFS snapshot deletion may delete renamed/moved files, which may result in data loss](#)

Known Issues in Apache Hive

Learn about the known issues in Hive, the impact or changes to the functionality, and the workaround.

CDPD-28809: error:java.lang.OutOfMemoryError: Java heap space while uploading a file to ABFS Exception in thread "main" java.lang.OutOfMemoryError: Java heap space at java.nio.HeapByteBuffer.<init>(HeapByteBuffer.java:57) at java.nio.ByteBuffer.allocate(ByteBuffer.java:335) at org.apache.hadoop.io.ElasticByteBufferPool.getBuffer(ElasticByteBufferPool.java:96) at org.apache.hadoop.fs.azurebfs.services.AbfsOutputStream.writeCurrentBufferToService(AbfsOutputStream.java:414) at org.apache.hadoop.fs.azurebfs.services.AbfsOutputStream.writeCurrentBufferToService(AbfsOutputStream.java:394) at org.apache.hadoop.fs.azurebfs.services.AbfsOutputStream.write(AbfsOutputStream.java:210) at org.apache.hadoop.fs.FSDataOutputStream\$PositionCache.write(FSDataOutputStream.java:62)

How upload works in ABFS: Max number of upload requests which can be queued is $2^4 * \text{num_available_processors}$. Every request will hold byte buffer of size ``fs.azure.write.request.size`` whose default is 8 MB. Thus if num_availaible processors is 8, total memory utilised will $2^4 * 8 * 8 = 512$ MB which can cause processes to go OOM.

1. Configure `fs.azure.write.request.size` to a preferably lower value for example 1 MB.

2. Reduce the number of max request which can be queued by configuring the parameter `fs.azure.write.max.requests.to.queue`
3. Allocate more memory to the process by setting high Xmx values.

CDPD-28809 For GCS: Error: error:java.lang.OutOfMemoryError: Java heap space while uploading a file to Google Cloud storage at java.lang.OutOfMemoryError.<init>(OutOfMemoryError.java:48) at com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.media.MediaHttpUploader.buildContentChunk(M
at
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.media.MediaHttpUploader.resumableUpload(Me
Local Variable: com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.http.GenericUrl#49
Local Variable: com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.http.HttpResponse#24 at
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.media.MediaHttpUploader.upload(MediaHttpUp
Local Variable: com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.http.GenericUrl#48 Local
Variable:
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.media.MediaHttpUploader#24
at
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.services.AbstractGoogleClientRequest.executeUnp
at
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.services.AbstractGoogleClientRequest.executeUnp
at
com.google.cloud.hadoop.repackaged.gcs.com.google.api.client.googleapis.services.AbstractGoogleClientRequest.execute(AB
Local Variable: com.google.cloud.hadoop.repackaged.gcs.com.google.api.services.storage.Storage
\$Objects\$Insert#24 at
com.google.cloud.hadoop.repackaged.gcs.com.google.cloud.hadoop.util.AbstractGoogleAsyncWriteChannel
\$UploadOperation.call(AbstractGoogleAsyncWriteChannel.java:318)

How upload works in ABFS: Every GCS output stream will create a byte buffer chunk size 64 MB, which can be configured via `fs.gs.outputstream.upload.chunk.size`. So if there are large number of streams getting created by a process, it will eat up lot of memory thus causing OOM issue. For example if there are 31 threads, total memory utilised will be $31 * 64 \text{ MB} = 1984 \text{ MB}$.

1. Configure `fs.gs.outputstream.upload.chunk.size` to a lower value preferably 1MB - 4 MB.
2. Allocate more memory to the process by setting high Xmx values.

CDPD-15518: ACID tables you write using the Hive Warehouse Connector cannot be read from an Impala virtual warehouse.

Read the tables from a Hive virtual warehouse or using Impala queries in Data Hub.

CDPD-13636: Hive job fails with OutOfMemory exception in the Azure DE cluster

Set the parameter `hive.optimize.sort.dynamic.partition.threshold=0`. Add this parameter in Cloudera Manager (Hive Service Advanced Configuration Snippet (Safety Valve) for `hive-site.xml`)

ENGESC-2214: Hiveserver2 and HMS service logs are not deleted

Update Hive log4j configurations. Hive -> Configuration -> HiveServer2 Logging
 Advanced Configuration Snippet (Safety Valve) Hive Metastore -> Configuration ->
 Hive Metastore Server Logging Advanced Configuration Snippet (Safety Valve) Add
 the following to the configurations: `appender.DRFA.strategy.action.type=DELETE`
`appender.DRFA.strategy.action.basepath=${log.dir}` `appender.DRFA.strategy.action.maxdepth=1`
`appender.DRFA.strategy.action.PathConditions.glob=${log.file}.*`
`appender.DRFA.strategy.action.PathConditions.type=IfFileName`
`appender.DRFA.strategy.action.PathConditions.nestedConditions.type=IfAccumulatedFileCount`
`appender.DRFA.strategy.action.PathConditions.nestedConditions.exceeds=same value as`
`appender.DRFA.strategy.max`

HiveServer Web UI displays incorrect data

If you enabled auto-TLS for TLS encryption, the HiveServer2 Web UI does not display the correct data in the following tables: Active Sessions, Open Queries, Last Max n Closed Queries

CDPD-11890: Hive on Tez cannot run certain queries on tables stored in encryption zones

This problem occurs when the Hadoop Key Management Server (KMS) connection is SSL-encrypted and a self signed certificate is used. SSLHandshakeException might appear in Hive logs.

Use one of the workarounds:

- Install a self signed SSL certificate into cacerts file on all hosts.
- Copy ssl-client.xml to a directory that is available in all hosts. In Cloudera Manager, in Clusters Hive on Tez Configuration . In Hive Service Advanced Configuration Snippet for hive-site.xml, click +, and add the name tez.aux.uris and valuepath-to-ssl-client.xml.

Technical Service Bulletins

TSB 2021-501: JOIN queries return wrong result for join keys with large size in Hive

JOIN queries return wrong results when performing joins on large size keys (larger than 255 bytes). This happens when the fast hash table join algorithm is enabled, which is enabled by default.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-501: JOIN queries return wrong result for join keys with large size in Hive](#)

TSB 2021-518: Incorrect results returned when joining two tables with different bucketing versions

Incorrect results are returned when joining two tables with different bucketing versions, and with the following Hive configurations: set hive.auto.convert.join = false and set mapreduce.job.reduces = any custom value.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-518: Incorrect results returned when joining two tables with different bucketing versions](#)

TSB 2021-520: Cleaner causes data loss when processing an aborted dynamic partitioning transaction

Data loss may occur when an operation that involves dynamic partitioning is aborted in Hive. Cleaner does not know what partition contains the aborted deltas, so it goes over all partitions and removes aborted and `obsolete` deltas below the HighWatermark (highest writeid that could be cleaned up). Those `obsolete` deltas may be `active` ones. There is no easy way to identify obsolete deltas that are active because HighWatermark is defined on a table level.

Upstream JIRA

[HIVE-25502](#)

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-520: Cleaner causes data loss when processing an aborted dynamic partitioning transaction](#)

TSB 2021-532: HWC fails to write empty DataFrame to orc files

HWC writes fail when an empty DataFrame write is attempted. That is because the writer does not create an orc file if no records are present in the DataFrame. This causes the HWC write commit validation to fail.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2021-532: HWC fails to write empty DataFrame to orc files](#)

TSB 2023-627: IN/OR predicate on binary column returns wrong result

An IN or an OR predicate involving a binary datatype column may produce wrong results. The OR predicate is converted to an IN due to the setting hive.optimize.point.lookup which is true by default. Only binary data types are affected by this issue. See <https://issues.apache.org/jira/browse/HIVE-26235> for example queries which may be affected.

Upstream JIRA

[HIVE-26235](#)

Knowledge article

For the latest update on this issue, see the corresponding Knowledge article: [TSB 2023-627: IN/OR predicate on binary column returns wrong result](#)

Known Issues in Hue

Learn about the known issues in Hue, the impact or changes to the functionality, and the workaround.

Downloading Impala query results containing special characters in CSV format fails with ASCII codec error

In CDP, Hue is compatible with Python 2.7.x, but the Tablib library for Hue has been upgraded from 0.10.x to 0.14.x, which is generally used with the Python 3 release. If you try to download Impala query results having special characters in the result set in a CSV format, then the download may fail with the ASCII unicode decode error.

To fix this issue, downgrade the Tablib library to 0.12.x.

1. SSH into the Hue server host.
2. Change directory to the following:

```
cd /opt/cloudera/parcels/CDH-7.x/lib/
```

3. Back up the hue directory:

```
cp -R hue hue_original
```

4. Change to the hue directory:

```
cd hue
```

5. Install the Wheel package using pip:

```
./build/env/bin/pip install wheel
```

The Wheel package is used to avoid recompiling your software during every install.

6. Install the Python Setuptools package for Hue as follows:

```
./build/env/bin/pip install setuptools==44.1.0
```

7. Install Tablib version 0.12.1 as follows:

```
./build/env/bin/pip install tablib==0.12.1
```

8. Go to Cloudera Manager and restart the Hue service.

Impala SELECT table query fails with UTF-8 codec error

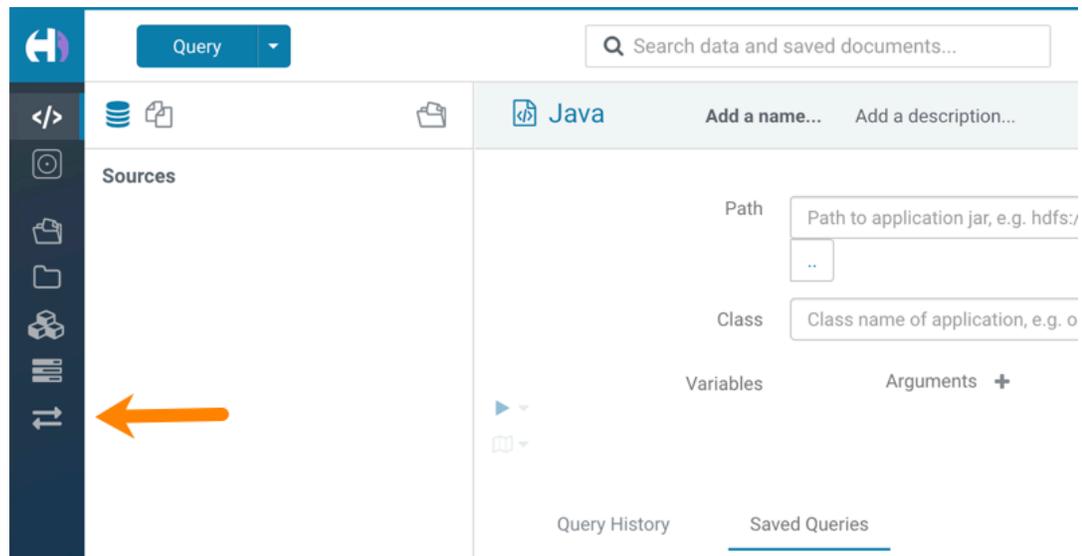
Hue cannot handle columns containing non-UTF8 data. As a result, you may see the following error while queying tables from the Impala editor in Hue: 'utf8' codec can't decode byte 0x91 in position 6: invalid start byte.

To resolve this issue, contact Cloudera Support to apply the following software patch: ENGESC-3457.

Hue Importer is not supported in the Data Engineering template

When you create a Data Hub cluster using the Data Engineering template, the Importer application is not supported in Hue.

Figure 1: Hue web UI showing Importer icon on the left assist panel



Hue Load Balancer role fails to start after upgrade to Cloudera Runtime 7 or you get the "BalancerMember worker hostname too long" error

You may see the following error message while starting the Hue Load Balancer:

```
BalancerMember worker hostname (xxx-xxxxxxxx-xxxxxxxxxxxx-xxxxxxx
.xxxxxx-xxxxxx-xxxxxx.example.site) too long.
```

Or, the Hue load balancer role fails to start after the upgrade, which prevents the Hue service from starting. If this failure occurs during cluster creation, cluster creation fails with the following error:

```
com.sequenceiq.cloudbreak.cm.ClouderaManagerOperationFailedException: Cluster template install failed: [Command [Start], with id [1234567890] failed: Failed to start role., Command [Start], with id [1234567890] failed: Failed to start role., Command [Start], with id [1234567890] failed: Failed to start role.]
Unable to generate configuration for HUE_SERVER
Role failed to start due to error com.cloudera.cmf.service.config.ConfigGenException: Unable to generate config file hue.ini
```

Cloudera Manager displays this error when you create a Data Hub cluster using the Data Engineering template and the Hue Load Balancer worker node name has exceeded 64 characters. In a CDP Public Cloud deployment, the system automatically generates the Load Balancer worker node name through AWS or Azure.

For example, if you specify `cdp-123456-scalecluster` as the cluster name, CDP creates `cdp-123456-scalecluster-master2.repro-aw.a123-4a5b.example.site` as the worker node name.

Specify a shorter cluster name while creating a Data Hub cluster so that the final worker node name does not cross 64 characters.

For example, `cdp-123456-scale`.

Unsupported features

Importing and exporting Oozie workflows across clusters and between different CDH versions is not supported

You can export Oozie workflows, schedules, and bundles from Hue and import them only within the same cluster if the cluster is unchanged. You can migrate bundle and coordinator jobs with their workflows only if their arguments have not changed between the old and the new cluster. For

example, hostnames, NameNode, Resource Manager names, YARN queue names, and all the other parameters defined in the workflow.xml and job.properties files.

Using the import-export feature to migrate data between clusters is not recommended. To migrate data between different versions of CDH, for example, from CDH 5 to CDP 7, you must take the dump of the Hue database on the old cluster, restore it on the new cluster, and set up the database in the new environment. Also, the authentication method on the old and the new cluster should be the same because the Oozie workflows are tied to a user ID, and the exact user ID needs to be present in the new environment so that when a user logs into Hue, they can access their respective workflows.



Note: Migrating Oozie workflows from HDP clusters is not supported.

Known Issues in Apache Impala

Learn about the known issues in Impala, the impact or changes to the functionality, and the workaround.

Impala known limitation when querying compacted tables

When the compaction process deletes the files for a table from the underlying HDFS location, the Impala service does not detect the changes as the compactions does not allocate new write ids. When the same table is queried from Impala it throws a 'File does not exist' exception that looks something like this:

```
Query Status: Disk I/O error on <node>:22000: Failed to open HDFS file hdfs://nameservice1/warehouse/tablespace/managed/hive/<database>/<table>/xxxxx
Error(2): No such file or directory Root cause: RemoteException: File does not exist: /warehouse/tablespace/managed/hive/<database>/<table>/xxxx
```

Use the [REFRESH/INVALIDATE](#) statements on the affected table to overcome the 'File does not exist' exception.

HADOOP-15720: Queries stuck on failed HDFS calls and not timing out

In Impala 3.2 and higher, if the following error appears multiple times in a short duration while running a query, it would mean that the connection between the impalad and the HDFS NameNode is in a bad state.

```
"hdfsOpenFile() for <filename> at backend <hostname:port> failed to finish before the <hdfs_operation_timeout_sec> second timeout"
```

In Impala 3.1 and lower, the same issue would cause Impala to wait for a long time or not respond without showing the above error message.

Restart the impalad.

IMPALA-532: Impala should tolerate bad locale settings

If the LC_* environment variables specify an unsupported locale, Impala does not start.

Add LC_ALL="C" to the environment settings for both the Impala daemon and the Statestore daemon.

IMPALA-5605: Configuration to prevent crashes caused by thread resource limits

Impala could encounter a serious error due to resource usage under very high concurrency. The error message is similar to:

```
F0629 08:20:02.956413 29088 llvm-codegen.cc:111] LLVM hit fatal error: Unable to allocate section memory!
```

```
terminate called after throwing an instance of 'boost::exception_
detail::clone_impl<boost::exception_detail::error_info_injector<
boost::thread_resource_error> >'
```

To prevent such errors, configure each host running an `impalad` daemon with the following settings:

```
echo 2000000 > /proc/sys/kernel/threads-max
echo 2000000 > /proc/sys/kernel/pid_max
echo 8000000 > /proc/sys/vm/max_map_count
```

Add the following lines in `/etc/security/limits.conf`:

```
impala soft nproc 262144
impala hard nproc 262144
```

IMPALA-635: Avro Scanner fails to parse some schemas

The default value in Avro schema must match type of first union type, e.g. if the default value is null, then the first type in the UNION must be "null".

Swap the order of the fields in the schema specification. For example, use `["null", "string"]` instead of `["string", "null"]`. Note that the files written with the problematic schema must be rewritten with the new schema because Avro files have embedded schemas.

IMPALA-691: Process mem limit does not account for the JVM's memory usage

Some memory allocated by the JVM used internally by Impala is not counted against the memory limit for the `impalad` daemon.

To monitor overall memory usage, use the `top` command, or add the memory figures in the Impala web UI `/memz` tab to JVM memory usage shown on the `/metrics` tab.

IMPALA-9350: Ranger audit logs for applying column masking policies missing

Impala is not producing these logs.

None

IMPALA-1024: Impala BE cannot parse Avro schema that contains a trailing semi-colon

If an Avro table has a schema definition with a trailing semicolon, Impala encounters an error when the table is queried.

Remove trailing semicolon from the Avro schema.

IMPALA-1652: Incorrect results with basic predicate on CHAR typed column

When comparing a CHAR column value to a string literal, the literal value is not blank-padded and so the comparison might fail when it should match.

Use the `RPAD()` function to blank-pad literals compared with CHAR columns to the expected length.

IMPALA-1792: ImpalaODBC: Can not get the value in the SQLGetData(m-x th column) after the SQLBindCol(m th column)

If the ODBC `SQLGetData` is called on a series of columns, the function calls must follow the same order as the columns. For example, if data is fetched from column 2 then column 1, the `SQLGetData` call for column 1 returns NULL.

Fetch columns in the same order they are defined in the table.

Test if a host is affected by checking whether the output of the `hostname` command includes the FQDN. On hosts where `hostname`, only returns the short name, pass the command-line flag `##hostname=fully_qualified_domain_name` in the startup options of all Impala-related daemons.

IMPALA-6671: Metadata operations block read-only operations on unrelated tables

Metadata operations that change the state of a table, like `COMPUTE STATS` or `ALTER RECOVER PARTITIONS`, may delay metadata propagation of unrelated unloaded tables triggered by statements like `DESCRIBE` or `SELECT` queries.

Workaround: None

IMPALA-7072: Impala does not support Heimdal Kerberos

CDPD-28139: Set spark.hadoop.hive.stats.autogather to false by default

As an Impala user, if you submit a query against a table containing data ingested using Spark and you are concerned about the quality of the query plan, you must run `COMPUTE STATS` against such a table in any case after an ETL operation because `numRows` created by Spark could be incorrect. Also, use other stats computed by `COMPUTE STATS`, e.g., Number of Distinct Values (NDV) and NULL count for good selectivity estimates.

For example, when a user ingests data from a file into a partition of an existing table using Spark, if `spark.hadoop.hive.stats.autogather` is not set to false explicitly, `numRows` associated with this partition would be 0 even though there is at least one row in the file. To avoid this, the workaround is to set `"spark.hadoop.hive.stats.autogather=false"` in the "Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf" in Spark's CM Configuration section.

Technical Service Bulletins

TSB 2021-479: Impala can return incomplete results through JDBC and ODBC clients in all CDP offerings

In CDP, we introduced a timeout on queries to Impala defaulting to 10 seconds. The timeout setting is called `FETCH_ROWS_TIMEOUT_MS`. Due to this setting, JDBC, ODBC, and Beeswax clients running Impala queries believe the data returned at 10 seconds is a complete dataset and present it as the final output. However, in cases where there are still results to return after this timeout has passed, when the driver closes the connection, based on the timeout, it results in a scenario where the query results are incomplete.

Upstream JIRA

[IMPALA-7561](#)

Knowledge article

For the latest update on this issue, see the corresponding Knowledge article: [TSB-2021 479: Impala can return incomplete results through JDBC and ODBC clients in all CDP offerings](#)

TSB 2022-543: Impala query with predicate on analytic function may produce incorrect results

Apache Impala may produce incorrect results for a query which has all of the following conditions:

- There are two or more analytic functions (for example, `row_number()`) in an inline view
- Some of the functions have partition-by expression while the others do not
- There is a predicate on the inline view's output expression corresponding to the analytic function

Upstream JIRA

[IMPALA-11030](#)

Knowledge article

For the latest update on this issue, see the corresponding Knowledge article: [TSB 2022-543: Impala query with predicate on analytic function may produce incorrect results](#)

Known Issues in Apache Kafka

Learn about the known issues in Apache Kafka, the impact or changes to the functionality, and the workaround.

Known Issues

OPSAPS-59553: SMM's bootstrap server config should be updated based on Kafka's listeners

SMM does not show any metrics for Kafka or Kafka Connect when multiple listeners are set in Kafka.

Workaround: SMM cannot identify multiple listeners and still points to bootstrap server using the default broker port (9093 for SASL_SSL). You would have to override bootstrap server URL (hostname:port as set in the listeners for broker) in the following path:

Cloudera Manager > SMM > Configuration > Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml > Save Changes > Restart SMM.

Topics created with the kafka-topics tool are only accessible by the user who created them when the deprecated --zookeeper option is used

By default all created topics are secured. However, when topic creation and deletion is done with the kafka-topics tool using the --zookeeper option, the tool talks directly to Zookeeper. Because security is the responsibility of ZooKeeper authorization and authentication, Kafka cannot prevent users from making ZooKeeper changes. As a result, if the --zookeeper option is used, only the user who created the topic will be able to carry out administrative actions on it. In this scenario Kafka will not have permissions to perform tasks on topics created this way.

Use kafka-topics with the --bootstrap-server option that does not require direct access to Zookeeper.

Certain Kafka command line tools require direct access to Zookeeper

The following command line tools talk directly to ZooKeeper and therefore are not secured via Kafka:

- kafka-reassign-partitions

None

The offsets.topic.replication.factor property must be less than or equal to the number of live brokers

The offsets.topic.replication.factor broker configuration is now enforced upon auto topic creation. Internal auto topic creation will fail with a GROUP_COORDINATOR_NOT_AVAILABLE error until the cluster size meets this replication factor requirement.

None

Requests fail when sending to a nonexistent topic with auto.create.topics.enable set to true

The first few produce requests fail when sending to a nonexistent topic with auto.create.topics.enable set to true.

Increase the number of retries in the producer configuration setting retries.

Custom Kerberos principal names cannot be used for kerberized ZooKeeper and Kafka instances

When using ZooKeeper authentication and a custom Kerberos principal, Kerberos-enabled Kafka does not start. You must disable ZooKeeper authentication for Kafka or use the default Kerberos principals for ZooKeeper and Kafka.

None

KAFKA-2561: Performance degradation when SSL is enabled

In some configuration scenarios, significant performance degradation can occur when SSL is enabled. The impact varies depending on your CPU, JVM version, Kafka configuration, and message size. Consumers are typically more affected than producers.

Configure brokers and clients with `ssl.secure.random.implementation = SHA1PRNG`. It often reduces this degradation drastically, but its effect is CPU and JVM dependent.

OPSAPS-43236: Kafka garbage collection logs are written to the process directory

By default Kafka garbage collection logs are written to the agent process directory. Changing the default path for these log files is currently unsupported.

None

Unsupported Features

The following Kafka features are not supported in Cloudera Data Platform:

- Only Java and .Net based clients are supported. Clients developed with C, C++, Python, and other languages are currently not supported.
- While Kafka Connect is available as part of Runtime, it is currently not supported in CDP Public Cloud. NiFi is a proven solution for batch and real time data loading that complement Kafka's message broker capability. For more information, see [Creating your first Flow Management cluster](#).
- The Kafka default authorizer is not supported. This includes setting ACLs and all related APIs, broker functionality, and command-line tools.

Limitations

Collection of Partition Level Metrics May Cause Cloudera Manager's Performance to Degrade

If the Kafka service operates with a large number of partitions, collection of partition level metrics may cause Cloudera Manager's performance to degrade.

If you are observing performance degradation and your cluster is operating with a high number of partitions, you can choose to disable the collection of partition level metrics.



Important: If you are using SMM to monitor Kafka or Cruise Control for rebalancing Kafka partitions, be aware that both SMM and Cruise Control rely on partition level metrics. If partition level metric collection is disabled, SMM will not be able to display information about partitions. In addition, Cruise Control will not operate properly.

Complete the following steps to turn off the collection of partition level metrics:

1. Obtain the Kafka service name:
 - a. In Cloudera Manager, Select the Kafka service.
 - b. Select any available chart, and select Open in Chart Builder from the configuration icon drop-down.
 - c. Find `$$SERVICENAME=` near the top of the display.
The Kafka service name is the value of `$$SERVICENAME`.
2. Turn off the collection of partition level metrics:
 - a. Go to HostsHosts Configuration.
 - b. Find and configure the Cloudera Manager Agent Monitoring Advanced Configuration Snippet (Safety Valve) configuration property.

Enter the following to turn off the collection of partition level metrics:

```
[KAFKA_SERVICE_NAME]_feature_send_broker_topic_partition_entity_update_enabled=false
```

Replace `[KAFKA_SERVICE_NAME]` with the service name of Kafka obtained in step 1. The service name should always be in lower case.

- c. Click Save Changes.

Known Issues in Apache Knox

Learn about the known issues in Knox, the impact or changes to the functionality, and the workaround.

CDPD-3125: Logging out of Atlas does not manage the external authentication

At this time, Atlas does not communicate a log-out event with the external authentication management, Apache Knox. When you log out of Atlas, you can still open the instance of Atlas from the same web browser without re-authentication.

To prevent additional access to Atlas, close all browser windows and exit the browser.

Known Issues in Apache Kudu

Learn about the known issues in Apache Kudu, the impact or changes to the functionality, and the workaround.

Kudu supports only coarse-grain authorization. Kudu does not yet support integration with Atlas.

None

Kudu HMS Sync is disabled and is not yet supported

None

Known Issues in Apache Oozie

Learn about the known issues in Oozie, the impact or changes to the functionality, and the workaround.

CDPD-29302: The Atlas lineage information is missing in case of HWC JDBC write.

None

CDPD-29297: HWC + Oozie issue: Cannot create PoolableConnectionFactory

Currently only Spark cluster mode is supported in the Oozie Spark Action with Hive Warehouse Connector (HWC).

Use Spark action in cluster mode.

```
<spark xmlns="uri:oozie:spark-action:1.0">
  ...
  <mode>cluster</mode>
  ...
</spark>
```

CDPD-26975: Using the ABFS / S3A connectors in an Oozie workflow where the operations are "secured" may trigger an IllegalArgumentException with the error message java.net.URISyntaxException: Relative path in absolute URI.

Set the following XML configuration in the Datahub cluster's Cloudera Manager:

1. In the Cloudera Manager Admin Console, go to the Oozie service.
2. Click the Configuration tab.
3. In the Oozie Server Advanced Configuration Snippet (Safety Valve) for oozie-site.xml field, set the following:

Set the following if you are using Amazon S3:

```
<property>
opAccessorService.fs.s3a</name>
tmp/s3a</value>
<name>oozie.service.Hado
<value>fs.s3a.buffer.dir=
```

```
</property>
```

Set the following if you are using ABFS:

```
<property>
  <name>oozie.service.HadoopAccessorService.fs.abfs</name>
  <value>fs.azure.buffer.dir=/tmp/abfs</value>
</property>
<property>
  <name>oozie.service.HadoopAccessorService.fs.abfss</name>
  <value>fs.azure.buffer.dir=/tmp/abfss</value>
</property>
```

4. Enter a Reason for change, and then click Save Change to commit the changes.
5. Restart the Oozie service.

Oozie jobs fail (gracefully) on secure YARN clusters when JobHistory server is down

If the JobHistory server is down on a YARN (MRv2) cluster, Oozie attempts to submit a job, by default, three times. If the job fails, Oozie automatically puts the workflow in a SUSPEND state.

When the JobHistory server is running again, use the resume command to inform Oozie to continue the workflow from the point at which it left off.

CDPD-5340: The resourceManager property defined in an Oozie workflow might not work properly if the workflow is submitted through Knox proxy.

An Oozie workflow defined to use the resourceManager property might not work as expected in situations when the workflow is submitted through Knox proxy.

Define the jobTracker property with the same value as that of the resourceManager property.

Unsupported Feature

The following Oozie features are currently not supported in Cloudera Data Platform:

- Non-support for Pig action (CDPD-1070)
- Conditional coordinator input logic

Cloudera does not support using Derby database with Oozie. You can use it for testing or debugging purposes, but Cloudera does not recommend using it in production environments. This could cause failures while upgrading from CDH to CDP.

BUG-123856: Upgrade fails while configuring Oozie server.

None

Known Issues in Apache Phoenix

There are no known issues for Phoenix in Cloudera Runtime 7.2.11.

Known Issues in Apache Ranger

Learn about the known issues in Ranger, the impact or changes to the functionality, and the workaround.

CDPD-3296: Audit files for Ranger plugin components do not appear immediately in S3 after cluster creation

For Ranger plugin components (Atlas, Hive, HBase, etc.), audit data is updated when the applicable audit file is rolled over. The default Ranger audit rollover time is 24 hours, so audit data appears 24 hours after cluster creation.

To see the audit logs in S3 before the default rollover time of 24 hours, use the following steps to override the default value in the Cloudera Manager safety valve for the applicable service.

1. On the Configuration tab in the applicable service, select Advanced under CATEGORY.
2. Click the + icon for the <service_name> Advanced Configuration Snippet (Safety Valve) for ranger-<service_name>-audit.xml property.
3. Enter the following property in the Name box:
xasecure.audit.destination.hdfs.file.rollover.sec.
4. Enter the desired rollover interval (in seconds) in the Value box. For example, if you specify 180, the audit log data is updated every 3 minutes.
5. Click Save Changes and restart the service.

CDPD-12644: Ranger Key Names cannot be reused with the Ranger KMS KTS service

Key names cannot be reused with the Ranger KMS KTS service. If the key name of a delete key is reused, the new key can be successfully created and used to create an encryption zone, but data cannot be written to that encryption zone.

Use only unique key names when creating keys.

CDPD-17962: Ranger roles do not work when you upgrade from any CDP Private Cloud Base to CDP Private cloud base. Roles which are created prior to upgrade work as expected, issue is only for new roles created post upgrade and authorization enforced via ranger policies wont work for these new roles. This behavior is only observed with the upgraded cluster; a newly installed cluster does not show this behavior.

There are two possible workarounds to resolve this issue:

1. Update database entries (Recommended):
 - `select * from x_ranger_global_state where state_name='RangerRole';`
 - `update x_ranger_global_state set app_data='{ "Version": "2" }' where state_name='RangerRole';`
- Or
2. Add a property in safety valve under ranger-admin-site which will bypass the `getAppDataVersion` method:

Known Issues in Schema Registry

There are no known issues for Schema Registry in Cloudera Runtime 7.2.11.

Known Issues in Cloudera Search

Learn about the known issues in Cloudera Search, the impact or changes to the functionality, and the workaround.

Known Issues

MapreduceIndexerTool performance problem in CDP

The reduce step of the MorphlineMapper task of the MapReduceIndexerTool (MRIT) can take very long to finish in CDPD. The reason of the slowness is merging norms without HDFS caching.

HDFS caching can not be enabled in the affected MRIT versions. Future MRIT releases will both allow controlling HDFS caching and will turn it on by default. For existing MRIT releases, the only known workaround is omitting norms. This disables length normalization for the field, saves some memory and improves MRIT execution times. Only full-text fields can benefit from norms. Norms are omitted for primitive (non-analyzed) types by default. (Norms were formerly also used for index-time boosting but this usage has been deprecated. Index-time boosting can be achieved using doc values fields instead.)

The downside of omitting norms is that document length will not play a role in result ranking. (With norms enabled, documents with a shorter matching field would be ranked higher than matching documents with a longer field.)

You can control norms in the schema using the `omitNorms` attribute in the `fieldType` elements. To eliminate the slowdown, you must add `omitNorms="true"` to all `fieldType` elements. It is also possible to selectively set this attribute on selected fields, which allows reducing the slowdown without completely eliminating it.

Indexing fails with `socketTimeout`

Starting from CDH 6.0, the HTTP client library used by Solr has a default socket timeout of 10 minutes. Because of this, if a single request sent from an indexer executor to Solr takes more than 10 minutes to be serviced, the indexing process fails with a timeout error.

This timeout has been raised to 24 hours. Nevertheless, there still may be use cases where even this extended timeout period proves insufficient.

If your `MapreduceIndexerTool` or `HBaseMapreduceIndexerTool` batch indexing jobs fail with a timeout error during the go-live (Live merge, `MERGEINDEXES`) phase (This means the merge takes longer than 24 hours).

Use the `--go-live-timeout` option where the timeout can be specified in milliseconds.

If the timeout occurs during Near real time (NRT) indexing, Cloudera suggests you try the following workarounds:

- Check the batch size of your indexing job. Sending too large batches to Solr might increase the time needed on the Solr server to process the incoming batch.
- If your indexing job uses `deleteByQuery` requests, consider using `deleteById` wherever possible as `deleteByQuery` involves a complex locking mechanism on the Solr side which makes processing the requests slower.
- Check the number of executors for your Spark Crunch Indexer job. Too many executors can overload the Solr service. You can configure the number of executors by using the `--mappers` parameter
- Check that your Solr installation is correctly sized to accommodate the indexing load, making sure that the number of Solr servers and the number of shards in your target collection are adequate.
- The socket timeout for the connection can be configured in the morphline file. Add the `solrClientSocketTimeout` parameter to the `solrLocator` command

Example

```
SOLR_LOCATOR :
{
  collection : test_collection
  zkHost : "zookeeper1.example.corp:2181/solr"
# 10 minutes in milliseconds
  solrClientSocketTimeout: 600000
  # Max number of documents to pass per RPC from morphline to
  Solr Server
  # batchSize : 10000
}
```

Splitshard operation on HDFS index checks local filesystem and fails

When performing a shard split on an index that is stored on HDFS, `SplitShardCmd` still evaluates free disk space on the local file system of the server where Solr is installed. This may cause the command to fail, perceiving that there is no adequate disk space to perform the shard split.

Run the following command to skip the check for sufficient disk space altogether:

- On nonsecure clusters:

```
curl 'http://[${**SOLR_SERVER_HOSTNAME**}]:8983/solr/admin/collections?action=SPLITSHARD&collection=[**COLLECTION_NAME**]&shard=[**SHARD_TO_SPLIT**]&skipFreeSpaceCheck=true'
```

- On secure clusters:

```
curl -k -u : --negotiate 'http://[${**SOLR_SERVER_HOSTNAME**}]:8985/solr/admin/collections?action=SPLITSHARD&collection=[**COLLECTION_NAME**]&shard=[**SHARD_TO_SPLIT**]&skipFreeSpaceCheck=true'
```

Replace `[**SOLR_SERVER_HOSTNAME**]` with a valid Solr server hostname, `[**COLLECTION_NAME**]` with the collection name, and `[**SHARD_TO_SPLIT**]` with the ID of the to split.

To verify that the command executed successfully, check overseer logs for a similar entry:

```
2021-02-02 12:43:23.743 INFO (OverseerThreadFactory-9-thread-5-processing-n:myhost.example.com:8983_solr) [c:example s:shard1] o.a.s.c.a.c.SplitShardCmd Skipping check for sufficient disk space
```

Lucene index handling limitation

The Lucene index can only be upgraded by one major version. Solr 8 will not open an index that was created with Solr 6 or earlier.

There is no workaround, you need to reindex collections.

Solr service with no added collections causes the upgrade process to fail

Upgrade fails while performing the bootstrap collections step of the `solr-upgrade.sh` script with the error message:

```
Failed to execute command Bootstrap Solr Collections on service Solr
```

if there are no collections present in Solr.

If there are no collections added to it, remove the Solr service from your cluster before you start the upgrade.

Collection Creation No Longer Supports Automatically Selecting A Configuration If Only One Exists

Before CDH 5.5.0, a collection could be created without specifying a configuration. If no `-c` value was specified, then:

- If there was only one configuration, that configuration was chosen.
- If the collection name matched a configuration name, that configuration was chosen.

Search now includes multiple built-in configurations. As a result, there is no longer a case in which only one configuration can be chosen by default.

Explicitly specify the collection configuration to use by passing `-c <configName>` to `solrctl collection --create`.

CrunchIndexerTool which includes Spark indexer requires specific input file format specifications

If the `--input-file-format` option is specified with `CrunchIndexerTool`, then its argument must be text, avro, or avroParquet, rather than a fully qualified class name.

None

The quickstart.sh file does not validate ZooKeeper and the NameNode on some operating systems.

The quickstart.sh file uses the timeout function to determine if ZooKeeper and the NameNode are available. To ensure this check can be complete as intended, the quickstart.sh determines if the operating system on which the script is running supports timeout. If the script detects that the operating system does not support timeout, the script continues without checking if the NameNode and ZooKeeper are available. If your environment is configured properly or you are using an operating system that supports timeout, this issue does not apply.

This issue only occurs in some operating systems. If timeout is not available, the quickstart continues and final validation is always done by the MapReduce jobs and Solr commands that are run by the quickstart.

Field value class guessing and Automatic schema field addition are not supported with the MapReduceIndexerTool nor with the HBaseMapReduceIndexerTool.

The MapReduceIndexerTool and the HBaseMapReduceIndexerTool can be used with a Managed Schema created via NRT indexing of documents or via the Solr Schema API. However, neither tool supports adding fields automatically to the schema during ingest.

Define the schema before running the MapReduceIndexerTool or HBaseMapReduceIndexerTool. In non-schemaless mode, define in the schema using the schema.xml file. In schemaless mode, either define the schema using the Solr Schema API or index sample documents using NRT indexing before invoking the tools. In either case, Cloudera recommends that you verify that the schema is what you expect, using the List Fields API command.

The Browse and Spell Request Handlers are not enabled in schemaless mode

The Browse and Spell Request Handlers require certain fields to be present in the schema. Since those fields cannot be guaranteed to exist in a Schemaless setup, the Browse and Spell Request Handlers are not enabled by default.

If you require the Browse and Spell Request Handlers, add them to the solrconfig.xml configuration file. Generate a non-schemaless configuration to see the usual settings and modify the required fields to fit your schema.

Enabling blockcache writing may result in unusable indexes.

It is possible to create indexes with solr.hdfs.blockcache.write.enabled set to true. Such indexes may appear corrupt to readers, and reading these indexes may irrecoverably corrupt indexes. Blockcache writing is disabled by default.

None

Users with insufficient Solr permissions may receive a "Page Loading" message from the Solr Web Admin UI.

Users who are not authorized to use the Solr Admin UI are not given a page explaining that access is denied to them, instead receive a web page that never finishes loading.

None

Using MapReduceIndexerTool or HBaseMapReduceIndexerTool multiple times may produce duplicate entries in a collection.

Repeatedly running the MapReduceIndexerTool on the same set of input files can result in duplicate entries in the Solr collection. This occurs because the tool can only insert documents and cannot update or delete existing Solr documents. This issue does not apply to the HBaseMapReduceIndexerTool unless it is run with more than zero reducers.

To avoid this issue, use HBaseMapReduceIndexerTool with zero reducers. This must be done without Kerberos.

Deleting collections might fail if hosts are unavailable.

It is possible to delete a collection when hosts that host some of the collection are unavailable. After such a deletion, if the previously unavailable hosts are brought back online, the deleted collection may be restored.

Ensure all hosts are online before deleting collections.

Unsupported Features

The following Solr features are currently not supported in Cloudera Data Platform:

- [Package Management System](#)
- [HTTP/2](#)
- [Solr SQL/JDBC](#)
- [Graph Traversal](#)
- [Cross Data Center Replication \(CDCR\)](#)
- [SolrCloud Autoscaling](#)
- HDFS Federation
- Saving search results
- Solr contrib modules (Spark, MapReduce and Lily HBase indexers are not contrib modules but part of the Cloudera Search product itself, therefore they are supported).

Known Issues in Apache Spark

Learn about the known issues in Spark, the impact or changes to the functionality, and the workaround.

CDPD-217: HBase/Spark connectors are not supported

The *Apache HBase Spark Connector* (hbase-connectors/spark) and the *Apache Spark - Apache HBase Connector* (shc) are not supported in the initial CDP release.

None

CDPD-3038: Launching pyspark displays several HiveConf warning messages

When pyspark starts, several Hive configuration warning messages are displayed, similar to the following:

```
19/08/09 11:48:04 WARN conf.HiveConf: HiveConf of name hive.vect
orized.use.checked.expressions does not exist
19/08/09 11:48:04 WARN conf.HiveConf: HiveConf of name hive.te
z.cartesian-product.enabled does not exist
```

These errors can be safely ignored.

CDPD-2650: Spark cannot write ZSTD and LZ4 compressed Parquet to dynamically partitioned tables

Use a different compression algorithm.

CDPD-3783: Cannot create databases from Spark

Attempting to create a database using Spark results in an error similar to the following:

```
org.apache.spark.sql.AnalysisException:
  org.apache.hadoop.hive.ql.metadata.HiveException: Me
taException(message:Permission denied: user [sparkuser] does not
have [ALL] privilege on [hdfs://ip-10-1-2-3.cloudera.site:8020/
tmp/spark/warehouse/spark_database.db]);
```

Create the database using Hive or Impala, or specify the external data warehouse location in the create command. For example:

```
sql("create database spark_database location '/warehouse/tablesp
ace/external/hive/spark_database.db' ")
```

Known Issues for Apache Sqoop

Learn about the known issues in Sqoop, the impact or changes to the functionality, and the workaround.

Using direct mode causes problems

Using direct mode has several drawbacks:

- Imports can cause intermittent an overlapping input split.
- Imports can generate duplicate data.
- Many problems, such as intermittent failures, can occur.
- Additional configuration is required.

Stop using direct mode. Do not use the `--direct` option in Sqoop import or export commands.

CDPD-3089: Avro, S3, and HCat do not work together properly

Importing an Avro file into S3 with HCat fails with Delegation Token not available.

Parquet columns inadvertently renamed

Column names that start with a number are renamed when you use the `--as-parquetfile` option to import data.

Prepend column names in Parquet tables with one or more letters or underscore characters.

Importing Parquet files might cause out-of-memory (OOM) errors

Importing multiple megabytes per row before initial-page-run check (ColumnWriter) can cause OOM. Also, rows that vary significantly by size so that the next-page-size check is based on small rows, and is set very high, followed by many large rows can also cause OOM.

None

Known issues in Streams Messaging Manager

Learn about the known issues for Streams Messaging Manager in Cloudera Runtime 7.2.11.

OPSAPS-59553: SMM's bootstrap server config should be updated based on Kafka's listeners

SMM does not show any metrics for Kafka or Kafka Connect when multiple listeners are set in Kafka.

SMM cannot identify multiple listeners and still points to bootstrap server using the default broker port (9093 for SASL_SSL). You would have to override bootstrap server URL (hostname:port as set in the listeners for broker). Add the bootstrap server details in SMM safety valve in the following path:

Cloudera Manager > SMM > Configuration > Streams Messaging Manager Rest Admin Server Advanced Configuration Snippet (Safety Valve) for streams-messaging-manager.yaml > Add the following value for bootstrap servers>Save Changes > Restart SMM.

```
streams.messaging.manager.kafka.bootstrap.servers=<comma-separated list of brokers>
```

OPSAPS-59597: SMM UI logs are not supported by Cloudera Manager

Cloudera Manager does not support the log type used by SMM UI.

View the SMM UI logs on the host.

OPSAPS-59828: SMM cannot connect to Schema Registry when TLS is enabled

When TLS is enabled, SMM by default cannot properly connect to Schema Registry. As a result, when viewing topics in the SMM Data Explorer with the deserializer key or value set to Avro, the following error messages are shown:

- Error deserializing key/value for partition [***PARTITION***] at offset [***OFFSET***]. If needed, please seek past the record to continue consumption.
- Failed to fetch value schema versions for topic : '[***TOPIC***]'.

In addition, the following certificate error will also be present the SMM log:

- javax.net.ssl.SSLHandshakeException: PKIX path building failed:...

Additional security properties must be set for SMM.

1. In Cloudera Manager, select the SMM service.
2. Go to Configuration.
3. Find and configure the SMM_JMX_OPTS property.

Add the following JVM SSL properties:

- `Djavax.net.ssl.trustStore=[***SMM TRUSTSTORE LOCATION***]`
- `Djavax.net.ssl.trustStorePassword=[***PASSWORD***]`

Known Issues in Streams Replication Manager

Learn about the known issues in Streams Replication Manager, the impact or changes to the functionality, and the workaround.

Known Issues

CDPD-22089: SRM does not sync re-created source topics until the offsets have caught up with target topic

Messages written to topics that were deleted and re-created are not replicated until the source topic reaches the same offset as the target topic. For example, if at the time of deletion and re-creation there are a 100 messages on the source and target clusters, new messages will only get replicated once the re-created source topic has 100 messages. This leads to messages being lost.

None

CDPD-14019: SRM may automatically re-create deleted topics

If `auto.create.topics.enable` is enabled, deleted topics are automatically recreated on source clusters.

Prior to deletion, remove the topic from the topic allowlist with the `srm-control` tool. This prevents topics from being re-created.

```
srm-control topics --source [SOURCE_CLUSTER] --target [TARGET_CLUSTER] --remove [TOPIC1][TOPIC2]
```

CDPD-11079: Blacklisted topics appear in the list of replicated topics

If a topic was originally replicated but was later disallowed (blacklisted), it will still appear as a replicated topic under the `/remote-topics` REST API endpoint. As a result, if a call is made to this endpoint, the disallowed topic will be included in the response. Additionally, the disallowed topic will also be visible in the SMM UI. However, its Partitions and Consumer Groups will be 0, its Throughput, Replication Latency and Checkpoint Latency will show N/A.

None

CDPD-60823: Configuring the SRM Client's secure storage is mandatory for unsecured environments

In an unsecured environment the `srm-control` tool should not need any additional configuration to run. However, due to an issue with the automatic generation of the default configuration, configuring the SRM Client's secure storage is mandatory for the `srm-control` tool. This is true even if none of the clusters that the tool connects to are secured.

If a secure storage is not configured, the tool will fail with the following `NullPointerException`:

```
java.lang.NullPointerException
at com.cloudera.dim.mirror.SecureConfigProvider.retrievePassword(
SecureConfigProvider.java:99)
at com.cloudera.dim.mirror.SecureConfigProvider.configure(SecureConfigProvider.java:113)
at org.apache.kafka.common.config.AbstractConfig.instantiateConfigProviders(AbstractConfig.java:533)
```

```

at org.apache.kafka.common.config.AbstractConfig.resolveConfigVariables(AbstractConfig.java:477)
at org.apache.kafka.common.config.AbstractConfig.<init>(AbstractConfig.java:107)
at org.apache.kafka.common.config.AbstractConfig.<init>(AbstractConfig.java:142)
at org.apache.kafka.connect.mirror.MirrorMakerConfig.<init>(MirrorMakerConfig.java:88)
at com.cloudera.dim.mirror.MirrorControlCommand$SourceTargetCommand.init(MirrorControlCommand.java:97)
at com.cloudera.dim.mirror.MirrorControlCommand.issueCommand(MirrorControlCommand.java:369)
at com.cloudera.dim.mirror.MirrorControlCommand.main(MirrorControlCommand.java:346)

```

Configure a secure storage password and set it as an environment variable in your CLI session before running the srm-control tool.

1. In Cloudera Manager, select the Streams Replication Manager service.
2. Go to Configuration.
3. Find and configure the SRM Client's Secure Storage Password property.

Take note of the password that you configure.

4. Click Save changes.
5. Restart the SRM service
6. SSH into one of the SRM hosts in your cluster.
7. Set the secure storage password as an environment variable.

```
export [***SECURE STORAGE ENV VAR***]=" [***SECURE STORAGE PASSWORD***]"
```

Replace `[***SECURE STORAGE ENV VAR***]` with the name of the environment variable you specified in Environment Variable Holding SRM Client's Secure Storage Password. Replace `[***SRM SECURE STORAGE PASSWORD***]` with the password you specified in SRM Client's Secure Storage Password. For example:

```
export SECURESTOREPASS="mypassword"
```

OPSAPS-61001: Saving configuration changes for SRM is not possible

Cloudera Manager incorrectly labels the SRM Client's Secure Storage Password property as mandatory. Moreover, it does not offer this property for configuration when SRM is installed with the Add Service Wizard.

As a result, it is possible to install and start SRM without configuring this property. However, in a case like this, making changes to SRM's configuration is not possible until the SRM Client's Secure Storage Password property is set.

Configure the SRM Client's Secure Storage Password property.



Important: Once the SRM Client's Secure Storage Password property is configured, you must set the password configured with the property as an environment variable in your CLI session before running the srm-control tool. The tool will fail to run if the password is not set as an environment variable. For more information see [Configuring srm-control](#).

OPSAPS-61814: Using the service dependency method to configure Kerberos enabled co-located clusters is not supported

Using the Streams Replication Manager Co-located Kafka Cluster Alias property to auto-configure the connection to a Kerberos enabled co-located Kafka cluster is not supported. In a case like this,

the generated JAAS configuration contains host-specific configuration. This causes SRM to fail to connect to the co-located Kafka cluster on other hosts.

Define your co-located Kafka clusters using Kafka credentials. For more information, see [Defining co-located Kafka clusters using Kafka credentials](#). Alternatively, use the Streams Replication Manager's Replication Configs property to configure the connection to the co-located Kafka clusters.

OPSAPS-63992: Rolling restart unavailable for SRM

Initiating a rolling restart for the SRM service is not possible. Consequently, performing a rolling upgrade of the SRM service is also not possible.

None

CDPD-31745: SRM Control fails to configure internal topic when target is earlier than Kafka 2.3

When the target Kafka cluster of a replication is earlier than version 2.3, the srm-control internal topic is created with an incorrect configuration (`cleanup.policy=compact`). This causes the srm-control topic to lose the replication filter records, causing issues in the replication.

After a replication is enabled where the target Kafka cluster is earlier than 2.3, manually configure all srm-control.[*SOURCE CLUSTER ALIAS*].internal topics in the target cluster to use `cleanup.policy=compact`.

CDPD-31235: Negative consumer group lag when replicating groups through SRM

SRM checkpointing reads the offset-syncs topic to create offset mappings for committed consumer group offsets. In some corner cases, it is possible that a mapping is not available in offset-syncs. In a case like this SRM simply copies the source offset, which might not be a valid offset in the replica topic.

One possible situation is if there is an empty topic in the source cluster with a non-zero end offset (for example, retention already removed the records), and a consumer group which has a committed offset set to the end offset. If replication is configured to start replicating this topic, it will not have an offset mapping available in offset-syncs (as the topic is empty), causing SRM to copy the source offset.

This can cause issues when automatic offset synchronization is enabled, as the consumer group offset can be potentially set to a high number. SRM never rewinds these offsets, so even when there is a correct offset mapping available, the offset will not be updated correctly.

After offset mappings are created, stop the consumers of the group and set the committed offsets of the group to the end of the topic on the target cluster with this command:

```
kafka-consumer-groups --bootstrap-server [***HOST***]:[***PORT***] --group [***GROUP***] --topic [***SOURCE CLUSTER ALIAS***].[***TOPIC***] --reset-offsets --to-latest --execute
```

Alternatively, set it to the beginning of the topic with this command:

```
kafka-consumer-groups --bootstrap-server [***HOST***]:[***PORT***] --group <group> --topic [***SOURCE CLUSTER ALIAS***].[***TOPIC***] --reset-offsets --to-earliest --execute
```

OPSAPS-62546: Kafka External Account SSL keypassword configuration is used incorrectly by SRM

When a Kafka External Account specifies a keystore that uses an SSL key password, SRM uses it as the `ssl.keystore.key` configuration. Due to using the incorrect `ssl.keystore.key` configuration, SRM will fail to load the keystore in certain cases.

Workaround: For the keystores used by the Kafka External Accounts, the SSL key password should match the SSL keystore password, and the SSL keystore key password should not be provided.

Alternatively, you can use the legacy connection configurations based on the `streams.replication.manager.configs` to specify the SSL key password.

Limitations

SRM cannot replicate Ranger authorization policies to or from Kafka clusters

Due to a limitation in the Kafka-Ranger plugin, SRM cannot replicate Ranger policies to or from clusters that are configured to use Ranger for authorization. If you are using SRM to replicate data to or from a cluster that uses Ranger, disable authorization policy synchronization in SRM. This can be achieved by clearing the Sync Topic Acls Enabled (`sync.topic.acls.enabled`) checkbox.

SRM cannot ensure the exactly-once semantics of transactional source topics

SRM data replication uses at-least-once guarantees, and as a result cannot ensure the exactly-once semantics (EOS) of transactional topics in the backup/target cluster.



Note: Even though EOS is not guaranteed, you can still replicate the data of a transactional source, but you must set `isolation.level` to `read_committed` for SRM's internal consumers. This can be done by adding `[***SOURCE CLUSTER ALIAS***]->[***TARGET CLUSTER ALIAS***].consumer.isolation.level=read_committed` to the Streams Replication Manager's Replication Configs SRM service property in Cloudera Manger.

SRM checkpointing is not supported for transactional source topics

SRM does not correctly translate checkpoints (committed consumer group offsets) for transactional topics. Checkpointing assumes that the offset mapping function is always increasing, but with transactional source topics this is violated. Transactional topics have control messages in them, which take up an offset in the log, but they are never returned on the consumer API. This causes the mappings to decrease, causing issues in the checkpointing feature. As a result of this limitation, consumer failover operations for transactional topics is not possible.

Known Issues in MapReduce and YARN

Learn about the known issues in Mapreduce and YARN, the impact or changes to the functionality, and the workaround.

Known Issues

COMPX-5817: Queue Manager UI will not be able to present a view of pre-upgrade queue structure. CM Store is not supported and therefore Yarn will not have any of the pre-upgrade queue structure preserved.

When a Data Hub cluster is deleted, all saved configurations are also deleted. All YARN configurations are saved in CM Store and this is yet to be supported in Data Hub and Cloudera Manager. Hence, the YARN queue structure also will be lost when a Data Hub cluster is deleted or upgraded or restored.

COMPX-5244: Root queue should not be enabled for auto-queue creation

After dynamic auto child creation is enabled for a queue using the YARN Queue Manager UI, you cannot disable it using the YARN Queue Manager UI. That can cause problem when you want to switch between resource allocation modes, for example from weight mode to relative mode. The YARN Queue Manager UI does not let you to switch resource allocation mode if there is at least one dynamic auto child creation enabled parent queue in your queue hierarchy.

If the dynamic auto child creation enabled parent queue is NOT the root or the `root.default` queue: Stop and remove the dynamic auto child creation enabled parent queue. Note that this stops and remove all of its child queues as well.

If the dynamic auto child creation enabled parent queue is the root or the root.default queue:
You cannot stop and remove neither the root nor the root.default queue. You have to change the configuration in the applicable configuration file:

1. In Cloudera Manager, navigate to YARN>>Configuration.
2. Search for capacity scheduler and find the Capacity Scheduler Configuration Advanced Configuration Snippet (Safety Valve) property.
3. Add the following configuration: `yarn.scheduler.capacity.<queue-path>.auto-queue-creation-v2.enabled=false` For example: `yarn.scheduler.capacity.root.default.auto-queue-creation-v2.enabled=false` Alternatively, you can remove the `yarn.scheduler.capacity.<queue-path>.auto-queue-creation-v2.enabled` property from the configuration file.
4. Restart the Resource Manager.

COMPX-5589: Unable to add new queue to leaf queue with partition capacity in Weight/Absolute mode

Scenario

1. User creates one or more partitions.
2. Assigns a partition to a parent with children
3. Switches to the partition to distribute the capacities
4. Creates a new child queue under one of the leaf queues but the following error is displayed:

```

Error :
2021-03-05 17:21:26,734 ERROR
com.cloudera.cpx.server.api.repositories.SchedulerRepository: Val
idation failed for Add queue
operation. Error message: CapacityScheduler configuration vali
dation failed:java.io.IOException:
Failed to re-init queues : Parent queue 'root.test2' have childr
en queue used mixed of weight
mode, percentage and absolute mode, it is not allowed, please do
uble check, details:
{Queue=root.test2.test2childNew, label= uses weight mode}. {Que
ue=root.test2.test2childNew,
label=partition uses percentage mode}

```

To create new queues under leaf queues without hitting this error, perform the following:

1. Switch to Relative mode
 2. Create the required queues
 3. Create the required partitions
 4. Assign partitions and set capacities
 5. Switch back to Weight mode
1. Create the entire queue structure
 2. Create the required partitions
 3. Assign partition to queues
 4. Set partition capacities

COMPX-5264: Unable to switch to Weight mode on creating a managed parent queue in Relative mode

In the current implementation, if there is an existing managed queue in Relative mode, then conversion to Weight mode is not be allowed.

To proceed with the conversion from Relative mode to Weight mode, there should not be any managed queues. You must first delete the managed queues before conversion. In Weight mode, a parent queue can be converted into managed parent queue.

COMPX-5549: Queue Manager UI sets maximum-capacity to null when you switch mode with multiple partitions

If you associate a partition with one or more queues and then switch the allocation mode before assigning capacities to the queues, an Operation Failed error is displayed as the `max-capacity` is set to null.

After you associate a partition with one or more queues, in the YARN Queue Manager UI, click Overview > <Partition name> from the dropdown list and distribute capacity to the queues before switching allocation mode or creating placement rules.

COMPX-4992: Unable to switch to absolute mode after deleting a partition using YARN Queue Manager

If you delete a partition (node label) which has been associated with queues and those queues have capacities configured for that partition (node label), the CS.xml still contains the partition (node label) information. Hence, you cannot switch to absolute mode after deleting the partition (node label).

It is recommended not to delete a partition (node label) which has been associated with queues and those queues have capacities configured for that partition (node label).

COMPX-3181: Application logs does not work for AZURE and AWS cluster

Yarn Application Log Aggregation will fail for any YARN job (MR, Tez, Spark, etc) which do not use cloud storage, or use a cloud storage location other than the one configured for YARN logs (`yarn.nodemanager.remote-app-log-dir`).

Configure the following:

- For MapReduce job, set `mapreduce.job.hdfs-servers` in the `mapred-site.xml` file with all filesystems required for the job including the one set in `yarn.nodemanager.remote-app-log-dir` such as `hdfs://nn1/`, `hdfs://nn2/`.
- For Spark job, set the job level with all filesystems required for the job including the one set in `yarn.nodemanager.remote-app-log-dir` such as `hdfs://nn1/`, `hdfs://nn2/` in `spark.yarn.access.hadoopFileSystems` and pass it through the `--config` option in `spark-submit`.
- For jobs submitted using the `hadoop` command, place a separate `core-site.xml` file with `fs.defaultFS` set to the filesystem set in `yarn.nodemanager.remote-app-log-dir` in a path. Add that directory path in `--config` when executing the `hadoop` command.

COMPX-1445: Queue Manager operations are failing when Queue Manager is installed separately from YARN

If Queue Manager is not selected during YARN installation, Queue Manager operation are failing. Queue Manager says 0 queues are configured and several failures are present. That is because ZooKeeper configuration store is not enabled.

1. In Cloudera Manager, select the YARN service.
2. Click the Configuration tab.
3. Find the Queue Manager Service property.
4. Select the Queue Manager service that the YARN service instance depends on.
5. Click Save Changes.
6. Restart all services that are marked stale in Cloudera Manager.

COMPX-1451: Queue Manager does not support multiple ResourceManagers

When YARN High Availability is enabled there are multiple ResourceManagers. Queue Manager receives multiple ResourceManager URLs for a High Availability cluster. It picks the active ResourceManager URL only when Queue Manager page is loaded. Queue Manager cannot handle it gracefully when the currently active ResourceManager goes down while the user is still using the Queue Manager UI.

Reload the Queue Manager page manually.

COMPX-3329: Autorestart is not enabled for Queue Manager in Data Hub

In a Data Hub cluster, Queue Manager is installed with autorestart disabled. Hence, if Queue Manager goes down, it will not restart automatically.

If Queue Manager goes down in a Data Hub cluster, you must go to the Cloudera Manager Dashboard and restart the Queue Manager service.

Third party applications do not launch if MapReduce framework path is not included in the client configuration

MapReduce application framework is loaded from HDFS instead of being present on the NodeManagers. By default the `mapreduce.application.framework.path` property is set to the appropriate value, but third party applications with their own configurations will not launch.

Set the `mapreduce.application.framework.path` property to the appropriate configuration for third party applications.

OPSAPS-57067: Yarn Service in Cloudera Manager reports stale configuration `yarn.cluster.scaling.recommendation.enable`.

This issue does not affect the functionality. Restarting Yarn service will fix this issue.

JobHistory URL mismatch after server relocation

After moving the JobHistory Server to a new host, the URLs listed for the JobHistory Server on the ResourceManager web UI still point to the old JobHistory Server. This affects existing jobs only. New jobs started after the move are not affected.

For any existing jobs that have the incorrect JobHistory Server URL, there is no option other than to allow the jobs to roll off the history over time. For new jobs, make sure that all clients have the updated `mapred-site.xml` that references the correct JobHistory Server.

CDH-49165: History link in ResourceManager web UI broken for killed Spark applications

When a Spark application is killed, the history link in the ResourceManager web UI does not work.

To view the history for a killed Spark application, see the Spark HistoryServer web UI instead.

CDH-6808: Routable IP address required by ResourceManager

ResourceManager requires routable host:port addresses for `yarn.resourcemanager.scheduler.address`, and does not support using the wildcard `0.0.0.0` address.

Set the address, in the form `host:port`, either in the client-side configuration, or on the command line when you submit the job.

OPSAPS-52066: Stacks under Logs Directory for Hadoop daemons are not accessible from Knox Gateway.

Stacks under the Logs directory for Hadoop daemons, such as NameNode, DataNode, ResourceManager, NodeManager, and JobHistoryServer are not accessible from Knox Gateway.

Administrators can SSH directly to the Hadoop Daemon machine to collect stacks under the Logs directory.

CDPD-2936: Application logs are not accessible in WebUI2 or Cloudera Manager

Running Containers Logs from NodeManager local directory cannot be accessed either in Cloudera Manager or in WebUI2 due to log aggregation.

Use the YARN log CLI to access application logs. For example:

```
yarn logs -applicationId <Application ID>
```

Apache Issue: [YARN-9725](#)

OPSAPS-50291: Environment variables `HADOOP_HOME`, `PATH`, `LANG`, and `TZ` are not getting whitelisted

It is possible to whitelist the environment variables `HADOOP_HOME`, `PATH`, `LANG`, and `TZ`, but the container launch environments do not have these variables set up automatically.

You can manually add the required environment variables to the whitelist using Cloudera Manager.

1. In Cloudera Manager, select the YARN service.

2. Click the Configuration tab.
3. Search for Containers Environment Variable Whitelist.
4. Add the environment variables (HADOOP_HOME, PATH, LANG, TZ) which are required to the list.
5. Click Save Changes.
6. Restart all NodeManagers.
7. Check the YARN aggregated logs to ensure that newly whitelisted environment variables are set up for container launch.

YARN cannot start if Kerberos principal name is changed

If the Kerberos principal name is changed in Cloudera Manager after launch, YARN will not be able to start. In such case the keytabs can be correctly generated but YARN cannot access ZooKeeper with the new Kerberos principal name and old ACLs.

There are two possible workarounds:

- Delete the znode and restart the YARN service.
- Use the reset ZK ACLs command. This also sets the znodes below /rmstore/ZKRMStateRoot to world:anyone:cdrwa which is less secure.

COMPX-8687: Missing access check for getAppAttempts

When the Job ACL feature is enabled using Cloudera Manager (YARN Configuration Enable JOB ACL property), the `mapreduce.cluster.acls.enabled` property is not generated to all configuration files, including the `yarn-site.xml` configuration file. As a result the ResourceManager process will use the default value of this property. The default property of `mapreduce.cluster.acls.enabled` is false.

Workaround: Enable the Job ACL feature using an advanced configuration snippet:

1. In Cloudera Manager select the YARN service.
2. Click Configuration.
3. Find the YARN Service MapReduce Advanced Configuration Snippet (Safety Valve) property.
4. Click the plus icon and add the following:
 - Name: `mapreduce.cluster.acls.enabled`
 - Value: `true`
5. Click Save Changes.

Unsupported Features

The following YARN features are currently not supported in Cloudera Data Platform:

- Application Timeline Server (ATSv2 and ATsv1)
- Container Resizing
- Distributed or Centralized Allocation of Opportunistic Containers
- Distributed Scheduling
- Docker on YARN (DockerContainerExecutor) on Data Hub clusters
- Fair Scheduler
- GPU support for Docker
- Hadoop Pipes
- Native Services
- Pluggable Scheduler Configuration
- Queue Priority Support
- Reservation REST APIs
- Resource Estimator Service
- Resource Profiles

- (non-Zookeeper) ResourceManager State Store
- Rolling Log Aggregation
- Shared Cache
- YARN Federation
- Moving jobs between queues

Known Issues in Apache Zeppelin

Learn about the known issues in Zeppelin, the impact or changes to the functionality, and the workaround.

CDPD-3090: Due to a configuration typo, functionality involving notebook repositories does not work

Due to a missing closing brace, access to the notebook repositories API is blocked by default.

From the CDP Management Console, go to Cloudera Manager for the cluster running Zeppelin. On the Zeppelin configuration page (Zeppelin serviceConfiguration), enter shiro urls in the Search field, and then add the missing closing brace to the notebook-repositories URL, as follows:

```
/api/notebook-repositories/** = authc, roles[{{zeppelin_admin_group}}]
```

Click Save Changes, and restart the Zeppelin service.

CDPD-2406: Logout button does not work

Clicking the Logout button in the Zeppelin UI logs you out, but then immediately logs you back in using SSO.

Close the browser.

Known Issues in Apache ZooKeeper

Learn about the known issues in Zookeeper, the impact or changes to the functionality, and the workaround.

Zookeeper-client does not use ZooKeeper TLS/SSL automatically

The command-line tool 'zookeeper-client' is installed to all Cloudera Nodes and it can be used to start the default Java command line ZooKeeper client. However even when ZooKeeper TLS/SSL is enabled, the zookeeper-client command connects to localhost:2181, without using TLS/SSL.

Manually configure the 2182 port, when zookeeper-client connects to a ZooKeeper cluster. The following is an example of connecting to a specific three-node ZooKeeper cluster using TLS/SSL:

```
CLIENT_JVMFLAGS="-Dzookeeper.clientCnxnSocket=org.apache.zookeeper.ClientCnxnSocketNetty -Dzookeeper.ssl.keyStore.location=<path to your configured keystore> -Dzookeeper.ssl.keyStore.password=<the password you configured for the keystore> -Dzookeeper.ssl.trustStore.location=<path to your configured truststore> -Dzookeeper.ssl.trustStore.password=<the password you configured for the truststore> -Dzookeeper.client.secure=true" zookeeper-client -server <your.zookeeper.server-1>:2182,<your.zookeeper.server-2>:2182,<your.zookeeper.server-3>:2182
```

Behavioral Changes In Cloudera Runtime 7.2.11

You can review the changes in certain features or functionalities of components that have resulted in a change in behavior from the previously released version to this version of Cloudera Runtime 7.2.11.

Behavioral Changes in Cloudera Search

Learn about the change in certain functionality of Cloudera Search that has resulted in a change in behavior from the previously released version to this version of Cloudera Runtime.

Summary:

Accessing Solr Admin UI in CDP clusters secured with Ranger

Previous behavior:

The Solr Admin UI was accessible for users with non-admin privileges.

New behavior

Only users with admin privileges can access the Solr Admin UI.

Summary:

Invalid Atomic Update operations now fail

Previous behavior:

Invalid Atomic Updates threw a warning message.

New behavior:

Invalid Atomic Updates fail with an Exception.

Summary:

Admin API address has changed

Previous behavior:

In Solr 7 both `curl -k --negotiate -u: "https://hostname -f :8985/solr/?op=GETDELEGATION TOKEN"` and `curl -k --negotiate -u: "https://hostname -f :8985/solr/admin?op=GETDELEGATION TOKEN"` commands worked.

New behavior

In Solr 8 only `curl -k --negotiate -u: "https://hostname -f :8985/solr/admin?op=GETDELEGATION TOKEN"` command (with the 'admin' string added) works.

Behavioral Changes in Apache Phoenix

Learn about the change in certain functionality of Apache Phoenix that has resulted in a change in behavior from the previously released version to this version of Cloudera Runtime.

Summary:

As a consequence of including the Apache Phoenix fix PHOENIX-5213, some libraries that are in the old shaded phoenix-client JARs are included in the new JAR without relocation. These libraries are shaded in the new JAR. For example, `com.google.protobuf` package is shaded in the new JAR.

New behavior:

If you use any of these JARs in your current deployment, you must explicitly add the newly shaded dependencies to your applications.

Deprecation Notices In Cloudera Runtime 7.2.11

Certain features and functionalities have been removed or deprecated in Cloudera Runtime 7.2.11. You must review these items to understand whether you must modify your existing configuration. You can also learn about the features that will be removed or deprecated in the future release to plan for the required changes.

Terminology

Items in this section are designated as follows:

Deprecated

Technology that Cloudera is removing in a future CDP release. Marking an item as deprecated gives you time to plan for removal in a future CDP release.

Moving

Technology that Cloudera is moving from a future CDP release and is making available through an alternative Cloudera offering or subscription. Marking an item as moving gives you time to plan for removal in a future CDP release and plan for the alternative Cloudera offering or subscription for the technology.

Removed

Technology that Cloudera has removed from CDP and is no longer available or supported as of this release. Take note of technology marked as removed since it can potentially affect your upgrade plans.

Removed Components and Product Capabilities

No components are deprecated or removed in this Cloudera Runtime release.

Please contact Cloudera Support or your Cloudera Account Team if you have any questions.

Deprecation notices in Apache Kudu

Certain features and functionality in Kudu are deprecated or removed in Cloudera Runtime 7.2.11. You must review these changes along with the information about the features in Kudu that will be removed or deprecated in a future release.

- The Flume sink has been migrated to the Apache Flume project and removed from Kudu. Users depending on the Flume integration can use the old kudu-flume jars or migrate to the Flume jars containing the Kudu sink.
- Support for Apache Sentry authorization has been deprecated and may be removed in the next release. Users depending on the Sentry integration should migrate to the Apache Ranger integration for authorization.
- Support for Python 2 has been deprecated and may be removed in the next release.
- Support for CentOS/RHEL 6, Debian 8, Ubuntu 14 has been deprecated and may be removed in the next release.

Deprecation Notices for Apache Kafka

Certain features and functionality in Apache Kafka are deprecated or removed in Cloudera Runtime 7.2.11. You must review these changes along with the information about the features in Kafka that will be removed or deprecated in a future release.

Deprecated

kafka-preferred-replica-election

The `kafka-preferred-replica-election.sh` command line tool has been deprecated in upstream Apache Kafka 2.4.0. Its alternative in CDP, `kafka-preferred.replica-election`, is also deprecated.

--zookeeper

The `--zookeeper` option has been deprecated for all Kafka command line tools except for `kafka-reassign-partitions`. Cloudera recommends that you use the `--bootstrap-server` option instead.

Deprecation Notices in Apache HBase

Certain features and functionality in HBase are deprecated or removed in Cloudera Runtime 7.2.11. You must review these changes along with the information about the features in HBase that will be removed or deprecated in a future release.

Use this list to understand some of the deprecated items and incompatibilities if you are upgrading from HDP 2.x or CDH 5.x to CDP.

Known Incompatibilities when Upgrading from CDH and HDP

Cloudera Runtime uses Apache HBase 2.x.x whereas CDH 5.x and HDP 2.x uses Apache HBase 1.x.



Important: Some APIs that are listed as deprecated, but these APIs do not block your upgrade. You must stop using the deprecated APIs in your existing applications after upgrade, and not use these APIs in new development.

List of Major Changes

- HBASE-16189 and HBASE-18945: You cannot open the Cloudera Runtime HFiles in CDH or HDP.
- HBASE-18240: Changed the ReplicationEndpoint Interface.
- The Dynamic Jars Directory property `hbase.dynamic.jars.dir` is disabled by default. If you want to enable dynamic classloading, you can use the `hbase.dynamic.jars.dir` property in Cloudera Manager to change the default `/${hbase.rootdir}/lib` directory to some other location, preferably a location on HDFS. This property is flagged by Cloudera Manager as deprecated when you upgrade to CDP because the property is incompatible with HBase on cloud deployments. If you are using HBase with HDFS storage, you can ignore this warning, and keep using the `hbase.use.dynamic.jars` feature.

Co-processor API changes

- HBASE-16769: Deprecated Protocol Buffers references from `MasterObserver` and `RegionServerObserver`.
- HBASE-17312: [JDK8] Use default method for Observer Coprocessors. The interface classes of `BaseMasterAndRegionObserver`, `BaseMasterObserver`, `BaseRegionObserver`, `BaseRegionServerObserver` and `BaseWALObserver` uses JDK8's 'default' keyword to provide empty and no-op implementations.
- Interface `HTableInterface` introduces following changes to the methods listed below:

[#] interface `CoprocessorEnvironment`

Change	Result
Abstract method <code>getTable (TableName)</code> has been removed.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>getTable (TableName, ExecutorService)</code> has been removed.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

- Public Audience

The following tables describes the coprocessor changes:

[#] class `CoprocessorRpcChannel` (1)

Change	Result
This class has become interface.	A client program may be interrupted by <code>IncompatibleClassChangeError</code> or <code>InstantiationException</code> exception depending on the usage of this class.

Class `CoprocessorHost<E>`

Classes that were Audience Private but were removed:

Change	Result
Type of field coprocessors has been changed from <code>java.util.SortedSet<E></code> to <code>org.apache.hadoop.hbase.util.SortedList<E></code> .	A client program may be interrupted by <code>NoSuchFieldError</code> exception.

MasterObserver changes

The following changes are introduced to the `MasterObserver` interface:

[#] interface `MasterObserver` (14)

Change	Result
Abstract method <code>voidpostCloneSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostCreateTable (ObserverContext<MasterCoprocesorEnvironment>, HTableDescriptor, HRegionInfo[])</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostDeleteSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostGetTableDescriptors (ObserverContext<MasterCoprocesorEnvironment>, List<HTableDescriptor>)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostModifyTable (ObserverContext<MasterCoprocesorEnvironment>, TableName, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostRestoreSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpostSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreCloneSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreCreateTable (ObserverContext<MasterCoprocesorEnvironment>, HTableDescriptor, HRegionInfo[])</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreDeleteSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreGetTableDescriptors (ObserverContext<MasterCoprocesorEnvironment>, List<TableName>, List<HTableDescriptor>)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreModifyTable (ObserverContext<MasterCoprocesorEnvironment>, TableName, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreRestoreSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>voidpreSnapshot (ObserverContext<MasterCoprocesorEnvironment>, HBaseProtos.SnapshotDescription, HTableDescriptor)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

RegionObserver interface changes

The following changes are introduced to the `RegionObserver` interface.

[#] interface RegionObserver (13)

Change	Result
Abstract method <code>void postCloseRegionOperation (ObserverContext<RegionCoprocesorEnvironment>, HRegion.Operation)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postCompactSelection (ObserverContext<RegionCoprocesorEnvironment>, Store, ImmutableList<StoreFile>)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postCompactSelection (ObserverContext<RegionCoprocesorEnvironment>, Store, ImmutableList<StoreFile>, CompactionRequest)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postGetClosestRowBefore (ObserverContext<RegionCoprocesorEnvironment>, byte[] , byte[] , Result)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>DeleteTracker postInstantiateDeleteTracker (ObserverContext<RegionCoprocesorEnvironment>, DeleteTracker)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postSplit (ObserverContext<RegionCoprocesorEnvironment>, HRegion, HRegion)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postStartRegionOperation (ObserverContext<RegionCoprocesorEnvironment>, HRegion.Operation)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>StoreFile.Reader postStoreFileReaderOpen (ObserverContext<RegionCoprocesorEnvironment>, FileSystem, Path, FSDataInputStreamWrapper, long, CacheConfig, Reference, StoreFile.Reader)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void postWALRestore (ObserverContext<RegionCoprocesorEnvironment>, HRegionInfo, HLogKey, WALEdit)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>InternalScanner preFlushScannerOpen (ObserverContext<RegionCoprocesorEnvironment>, Store, KeyValueScanner, InternalScanner)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void preGetClosestRowBefore (ObserverContext<RegionCoprocesorEnvironment>, byte[] , byte[] , Result)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>StoreFile.Reader preStoreFileReaderOpen (ObserverContext<RegionCoprocesorEnvironment>, FileSystem, Path, FSDataInputStreamWrapper, long, CacheConfig, Reference, StoreFile.Reader)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>void preWALRestore (ObserverContext<RegionCoprocesorEnvironment>, HRegionInfo, HLogKey, WALEdit)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

WALObserver interface changes

The following changes are introduced to the WALObserver interface:

[#] interface WALObserver

Change	Result
Abstract method <code>void postWALWrite (ObserverContext<WALCoprocesorEnvironment>, HRegionInfo, HLogKey, WALEdit)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>boolean preWALWrite (ObserverContext<WALCoprocesorEnvironment>, HRegionInfo, HLogKey, WALEdit)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

Scheduler changes

Following methods are now changed to abstract:

[#]class RpcScheduler (1)

Change	Result
Abstract method void dispatch (CallRunner) has been removed from this class.	A client program may be interrupted by NoSuchMethodError exception.

[#] RpcScheduler.dispatch (CallRunner p1) [abstract] : void 1

org/apache/hadoop/hbase/ipc/RpcScheduler.dispatch:(Lorg/apache/hadoop/hbase/ipc/CallRunner;)V

Change	Result
Return value type has been changed from void to boolean.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

The following abstract methods have been removed:

[#]interface PriorityFunction (2)

Change	Result
Abstract method longgetDeadline (RPCProtos.RequestHeader, Message) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method int getPriority (RPCProtos.RequestHeader, Message) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.

Server API changes

[#] class RpcServer (12)

Change	Result
Type of field CurCall has been changed from java.lang.ThreadLocal<RpcServer.Call> to java.lang.ThreadLocal<RpcCall>.	A client program may be interrupted by NoSuchFieldError exception.
Abstract method int getNumOpenConnections () has been added to this class.	This class became abstract and a client program may be interrupted by InstantiationException exception.
Field callQueueSize of type org.apache.hadoop.hbase.util.Counter has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field connectionList of type java.util.List<RpcServer.Connection> has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field maxIdleTime of type int has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field numConnections of type int has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field port of type int has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field purgeTimeout of type long has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field responder of type RpcServer.Responder has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field socketSendBufferSize of type int has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field thresholdIdleConnections of type int has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.

Following abstract methods are removed:

Change	Result
--------	--------

Abstract method Pair<Message,CellScanner>call (BlockingService, Descriptors.MethodDescriptor, Message, CellScanner, long, MonitoredRPCHandler) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
--	---

Replication and WAL changes

HBASE-18733: WALKey has been purged completely. Following are the changes to the WALKey:

[#] classWALKey (8)

Change	Result
Access level of field clusterIds has been changed from protected to private.	A client program may be interrupted by IllegalAccessException exception.
Access level of field compressionContext has been changed from protected to private.	A client program may be interrupted by IllegalAccessException exception.
Access level of field encodedRegionName has been changed from protected to private.	A client program may be interrupted by IllegalAccessException exception.
Access level of field tablename has been changed from protected to private.	A client program may be interrupted by IllegalAccessException exception.
Access level of field writeTime has been changed from protected to private.	A client program may be interrupted by IllegalAccessException exception.

Following fields have been removed:

Change	Result
Field LOG of type org.apache.commons.logging.Log has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field VERSION of type WALKey.Version has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field logSeqNum of type long has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.

Admin Interface API changes

You cannot administer a CDP Runtime Data Hub cluster using a client that includes RelicationAdmin, ACC, Thrift and REST usage of Admin ops. Methods returning protobufs have been changed to return POJOs instead. Returns have changed from void to Future for async methods. HBASE-18106 - Admin.listProcedures and Admin.listLocks were renamed to getProcedures and getLocks. MapReduce makes use of Admin doing following admin.getClusterStatus() to calculate Splits.

- Thrift usage of Admin API:

```
compact(ByteBuffer) createTable(ByteBuffer, List<ColumnDescriptor>) deleteTable(ByteBuffer) disableTable(ByteBuffer) enableTable(ByteBuffer) getTableNames() majorCompact(ByteBuffer)
```

- REST usage of Admin API:

```
hbase-rest org.apache.hadoop.hbase.rest RootResource getTableList() TableName[] tableNames = servlet.getAdmin().listTableNames(); SchemaResource delete(UriInfo) Admin admin = servlet.getAdmin(); update(TableNameSchemaModel, boolean, UriInfo) Admin admin = servlet.getAdmin(); StorageClusterStatusResource get(UriInfo) ClusterStatus status = servlet.getAdmin().getClusterStatus(); StorageClusterVersionResource get(UriInfo) model.setVersion(servlet.getAdmin().getClusterStatus().getHBaseVersion()); TableResource exists() return servlet.getAdmin().tableExists(TableName.valueOf(table));
```

[#] interface Admin (9)

Following are the changes to the Admin interface:

Change	Result
Abstract method <code>createTableAsync (HTableDescriptor, byte[][])</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>disableTableAsync (TableName)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>enableTableAsync (TableName)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>getCompactionState (TableName)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>getCompactionStateForRegion (byte[])</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>isSnapshotFinished (HBaseProtos.SnapshotDescription)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>snapshot (String, TableName, HBaseProtos.SnapshotDescription.Type)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>snapshot (HBaseProtos.SnapshotDescription)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.
Abstract method <code>takeSnapshotAsync (HBaseProtos.SnapshotDescription)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

[#] `Admin.createTableAsync (HTableDescriptor p1, byte[][] p2) [abstract] : void 1`

`org/apache/hadoop/hbase/client/Admin.createTableAsync:(Lorg/apache/hadoop/hbase/HTableDescriptor;[[B)V`

Change	Result
Return value type has been changed from <code>void</code> to <code>java.util.concurrent.Future<java.lang.Void></code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

[#] `Admin.disableTableAsync (TableName p1) [abstract] : void 1`

`org/apache/hadoop/hbase/client/Admin.disableTableAsync:(Lorg/apache/hadoop/hbase/TableName;)V`

Change	Result
Return value type has been changed from <code>void</code> to <code>java.util.concurrent.Future<java.lang.Void></code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

`Admin.enableTableAsync (TableName p1) [abstract] : void 1`

`org/apache/hadoop/hbase/client/Admin.enableTableAsync:(Lorg/apache/hadoop/hbase/TableName;)V`

Change	Result
Return value type has been changed from <code>void</code> to <code>java.util.concurrent.Future<java.lang.Void></code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

`Admin.enableTableAsync (TableName p1) [abstract] : void 1`

`org/apache/hadoop/hbase/client/Admin.getCompactionState:(Lorg/apache/hadoop/hbase/TableName;)Lorg/apache/hadoop/hbase/protobuf/generated/AdminProtos$GetRegionInfoResponse$CompactionState;`

Change	Result
Return value type has been changed from <code>org.apache.hadoop.hbase.protobuf.generated.AdminProtos.GetRegionInfoResponse.CompactionState</code> to <code>CompactionState</code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

[#] Admin.getCompactionStateForRegion (byte [] p1) [abstract] : AdminProtos.GetRegionInfoResponse.CompactionState 1

org/apache/hadoop/hbase/client/Admin.getCompactionStateForRegion:([B]Lorg/apache/hadoop/hbase/protobuf/generated/AdminProtos\$GetRegionInfoResponse\$CompactionState;

Change	Result
Return value type has been changed from org.apache.hadoop.hbase.protobuf.generated.AdminProtos.GetRegionInfoResponse.CompactionState to CompactionState.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

HTableDescriptor and HColumnDescriptor changes

HTableDescriptor and HColumnDescriptor has become interfaces and you can create it through Builders. HCD has become CFD. It no longer implements writable interface. package org.apache.hadoop.hbase.

[#] class HColumnDescriptor (1)

Change	Result
Removed super-interface org.apache.hadoop.io.WritableComparable<HColumnDescriptor>.	A client program may be interrupted by NoSuchMethodError exception.

class HTableDescriptor (3)

Change	Result
Removed super-interface org.apache.hadoop.io.WritableComparable<HTableDescriptor>.	A client program may be interrupted by NoSuchMethodError exception.
Field META_TABLEDESC of type HTableDescriptor has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.

[#] HTableDescriptor.getColumnFamilies () : HColumnDescriptor [] (1)

org/apache/hadoop/hbase/HTableDescriptor.getColumnFamilies:()[Lorg/apache/hadoop/hbase/HColumnDescriptor;

[#] class HColumnDescriptor (1)

Change	Result
Return value type has been changed from HColumnDescriptor[] to client.ColumnFamilyDescriptor[].	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

[#] interface Table (4)

Change	Result
Abstract method batch (List<?>) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method batchCallback (List<?>, Batch.Callback<R>) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method getWriteBufferSize () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method setWriteBufferSize (long) has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.

Deprecated buffer methods

- LockTimeoutException and OperationConflictException classes have been removed.

class OperationConflictException (1)

Result	Result
This class has been removed.	A client program may be interrupted by NoClassDefFoundError exception.

class class LockTimeoutException (1)

Change Result This class has been removed. A client program may be interrupted by NoClassDefFoundError exception.

Filter API changes

Following methods have been removed: package org.apache.hadoop.hbase.filter

[#] class Filter (2)

Result	Result
Abstract method getNextKeyHint (KeyValue) has been removed from this class.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method transform (KeyValue) has been removed from this class.	A client program may be interrupted by NoSuchMethodError exception.

- HBASE-12296: Filters should work with ByteBufferedCell.
- HConnection is removed in Cloudera Runtime.
- RegionLoad and ServerLoad internally moved to shaded Protocol Buffers.

[#] class RegionLoad (1)

Result	Result
Type of field regionLoadPB has been changed from protobuf.generated.ClusterStatusProtos.RegionLoad to shaded.protobuf.generated.ClusterStatusProtos.RegionLoad.	A client program may be interrupted by NoSuchFieldError exception.

[#] interface AccessControlConstants (3)

Result	Result
Field OP_ATTRIBUTE_ACL_STRATEGY of type java.lang.String has been removed from this interface.	A client program may be interrupted by NoSuchFieldError exception.
Field OP_ATTRIBUTE_ACL_STRATEGY_CELL_FIRST of type byte[] has been removed from this interface.	A client program may be interrupted by NoSuchFieldError exception.
Field OP_ATTRIBUTE_ACL_STRATEGY_DEFAULT of type byte[] has been removed from this interface.	A client program may be interrupted by NoSuchFieldError exception.

[#] ServerLoad.getNumberOfRequests () : int 1

org/apache/hadoop/hbase/ServerLoad.getNumberOfRequests():I

Result	Result
Return value type has been changed from int to long.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

[#] ServerLoad.getNumberOfRequests () : int 1

org/apache/hadoop/hbase/ServerLoad.getReadRequestsCount():I

Result	Result
Return value type has been changed from int to long.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

[#] ServerLoad.getTotalNumberOfRequests () : int 1

org/apache/hadoop/hbase/ServerLoad.getTotalNumberOfRequests:()I

Result	Result
Return value type has been changed from int to long.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

[#]ServerLoad.getWriteRequestsCount () : int 1

org/apache/hadoop/hbase/ServerLoad.getWriteRequestsCount:()I

Result	Result
Return value type has been changed from int to long.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.

[#]class HConstants (6)

Result	Result
Field DEFAULT_HBASE_CONFIG_READ_ZOOKEEPER_CONFIG of type boolean has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field HBASE_CONFIG_READ_ZOOKEEPER_CONFIG of type java.lang.String has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field REPLICATION_ENABLE_DEFAULT of type boolean has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field REPLICATION_ENABLE_KEY of type java.lang.String has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field ZOOKEEPER_CONFIG_NAME of type java.lang.String has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.
Field ZOOKEEPER_USEMULTI of type java.lang.String has been removed from this class.	A client program may be interrupted by NoSuchFieldError exception.

HBASE-18732: [compat 1-2] HBASE-14047 removed Cell methods without deprecation cycle.

[#]interface Cell 5

Result	Result
Abstract method getFamily () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method getMvccVersion () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method getQualifier () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method getRow () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.
Abstract method getValue () has been removed from this interface.	A client program may be interrupted by NoSuchMethodError exception.

HBASE-18795:Expose KeyValue.getBuffer() for tests alone. Allows KV#getBuffer in tests only that was deprecated previously.

Region scanner changes

[#]interface RegionScanner (1)

Result	Result
Abstract method <code>boolean nextRaw (List<Cell>, int)</code> has been removed from this interface.	A client program may be interrupted by <code>NoSuchMethodError</code> exception.

StoreFile changes

[#] class StoreFile (1)

Result	Result
This class became interface.	A client program may be interrupted by <code>IncompatibleClassChangeError</code> or <code>InstantiationError</code> exception dependent on the usage of this class.

MapReduce changes

HFile*Format has been removed.

ClusterStatus changes

[#] ClusterStatus.getRegionsInTransition () : Map<String,RegionState> 1

org/apache/hadoop/hbase/ClusterStatus.getRegionsInTransition:()Ljava/util/Map;

Result	Result
Return value type has been changed from <code>java.util.Map<java.lang.String,master.RegionState></code> to <code>java.util.List<master.RegionState></code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

Other changes in ClusterStatus include removal of convert methods that were no longer necessary after purge of Protocol Buffers from API.

Purge of Protocol Buffers from API

Protocol Buffers (PB) has been deprecated in APIs.

[#] HBaseSnapshotException.getSnapshotDescription () : HBaseProtos.SnapshotDescription 1

org/apache/hadoop/hbase/snapshot/HBaseSnapshotException.getSnapshotDescription:()Lorg/apache/hadoop/hbase/protobuf/generated/HBaseProtos\$SnapshotDescription;

Result	Result
Return value type has been changed from <code>org.apache.hadoop.hbase.protobuf.generated.HBaseProtos.SnapshotDescription</code> to <code>org.apache.hadoop.hbase.client.SnapshotDescription</code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

HBASE-15609: Remove PB references from Result, DoubleColumnInterpreter and any such public facing class for 2.0. hbase-client-1.0.0.jar, Result.class package org.apache.hadoop.hbase.client

[#] Result.getStats () : ClientProtos.RegionLoadStats 1

org/apache/hadoop/hbase/client/Result.getStats:()Lorg/apache/hadoop/hbase/protobuf/generated/ClientProtos\$RegionLoadStats;

Result	Result
Return value type has been changed from <code>org.apache.hadoop.hbase.protobuf.generated.ClientProtos.RegionLoadStats</code> to <code>RegionLoadStats</code> .	This method has been removed because the return type is part of the method signature. A client program may be interrupted by <code>NoSuchMethodError</code> exception.

PrettyPrinter changes

hbase-server-1.0.0.jar, HFilePrettyPrinter.class package org.apache.hadoop.hbase.io.hfile

Result	Result
Return value type has been changed from void to int.	This method has been removed because the return type is part of the method signature. A client program may be interrupted by NoSuchMethodError exception.