Cloudera Runtime 7.2.11

Managing Apache Phoenix Security

Date published: 2020-02-29
Date modified: 2023-05-09

https://docs.cloudera.com/

Legal Notice

Contents

Phoenix is FIPS compliant

Phoenix is now Federal Information Processing Standards (FIPS) compliant.

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors. Phoenix Query Server (PQS) is compatible with an FIPS-enabled environment..

PQS can run on an OS with FIPS turned on and can use FIPS-compliant crypto libraries.

OMID is also compatible with an FIPS-enabled environment.

For more information, see *Installing and Configuring Cloudera with FIPS*.

Related Information

Installing and Configuring Cloudera with FIPS

Managing Apache Phoenix security

Apache Ranger manages authorization and access control through a user interface that ensures consistent policy administration for both Apache Phoenix and Apache HBase.

Apache Phoenix namespaces, tables, column family, and columns use the same access control parameters set in Apache HBase. You must first enable Apache Phoenix ACLs support using Cloudera Manager before you can define permissions for your Apache HBase tables if you are using Apache HBase ACLs.

Cloudera Shared Data Experience Data Lake helps you configure and manage authorization and access control through the Apache Ranger user interface that ensures consistent policy administration for Apache HBase. Apache Phoenix security derives policies applied to the underlying Apache HBase tables in Ranger. You can grant read or write permissions to an Apache HBase table for a specific user using the Apache Ranger user interface.

Auto-TLS is enabled by default in Cloudera. But you can also manually configure TLS for Phoenix Query Server. See the related inforamtion section to learn more about security in Cloudera.

Related Information

Configure TLS encryption manually for Phoenix Query Server

Cloudera Security

Enable Phoenix ACLs

To enable Phoenix ACLs using Cloudera Manager, edit the HBase Service advanced configuration snippet for the cluster.

Procedure

1. Go to the HBase service.
2. Click Configuration.
3. Search for the property HBase Service Advanced Configuration Snippet (Safety Valve) for hbase-site.xml.
4. Paste your configuration into the Value field and save your changes.

```
<property>
    <name>phoenix.acls.enabled</name>
    <value>true</value>
```

```
  </property>
```

5. Restart your cluster for the changes to take effect.

Configure TLS encryption manually for Phoenix Query Server

You can encrypt communication between clients and the Phoenix Query Server using Transport Layer Security (TLS) formerly known as Secure Socket Layer (SSL). You must follow these steps to manually configure TLS for Phoenix Query Server.

Before you begin

- Keystores containing certificates bound to the appropriate domain names must be accessible on all hosts running the Phoenix Query Server role of the Phoenix service.
- Keystores for Phoenix must be owned by the phoenix group, and have 0440 file permissions (that is, the file must be readable by the owner and group).
- Absolute paths to the keystore and truststore files must be specified. These settings apply to all hosts on which daemon roles of the Phoenix service run. Therefore, the paths you choose must be valid on all hosts.
- The Cloudera Manager version must support the TLS/SSL configuration for Phoenix at the service level. Ensure you specify absolute paths to the keystore and truststore files. These settings apply to all hosts on which daemon roles of the service in question run. Therefore, the paths you choose must be valid on all hosts.

  An implication of this is that the keystore file names for a given service must be the same on all hosts. If, for example, you have obtained separate certificates for Phoenix daemons on hosts node1.example.com and node2.example.com, you might have chosen to store these certificates in files called phoenix-node1.keystore and phoenix-node2.keystore (respectively). When deploying these keystores, you must give them both the same name on the target host — for example, phoenix.keystore.

Procedure

1. In Cloudera Manager, select the Phoenix service.
2. Click the Configuration tab.
3. Use the Scope / Query Server filter.
4. Search for tls.
5. Select Enable TLS/SSL for Query Server.
6. Edit the following TLS/SSL properties according to your configuration.

Table 1:

Property	Description
Query Server TLS/SSL Server JKS Keystore File Location	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Query Server is acting as a TLS/SSL server. The keystore must be in JKS format.
Query Server TLS/SSL Server JKS Keystore File Password	The password for the Query Server JKS keystore file.
Query Server TLS/SSL Client Trust Store File	The location on disk of the truststore file, in .jks format, used to confirm the authenticity of TLS/SSL servers to which the Query Server might connect. This is used when Query Server is the client in a TLS/SSL connection. This truststore file must contain the certificate(s) used to sign the connected service(s). If this parameter is not specified, the default list of known certificate authorities is used instead.

Property	Description
Query Server TLS/SSL Client Trust Store Password	The password for the Query Server TLS/SSL Certificate Trust Store File. This password is not mandatory to access the truststore; this field is optional. This password provides optional integrity checking of the file. The contents of truststores are certificates, and certificates are public information.

7. Click Save Changes.
8. Restart the Phoenix service.

Related Information

Managing Apache Phoenix security