

mod16_ex03: Verify Auto-TLS

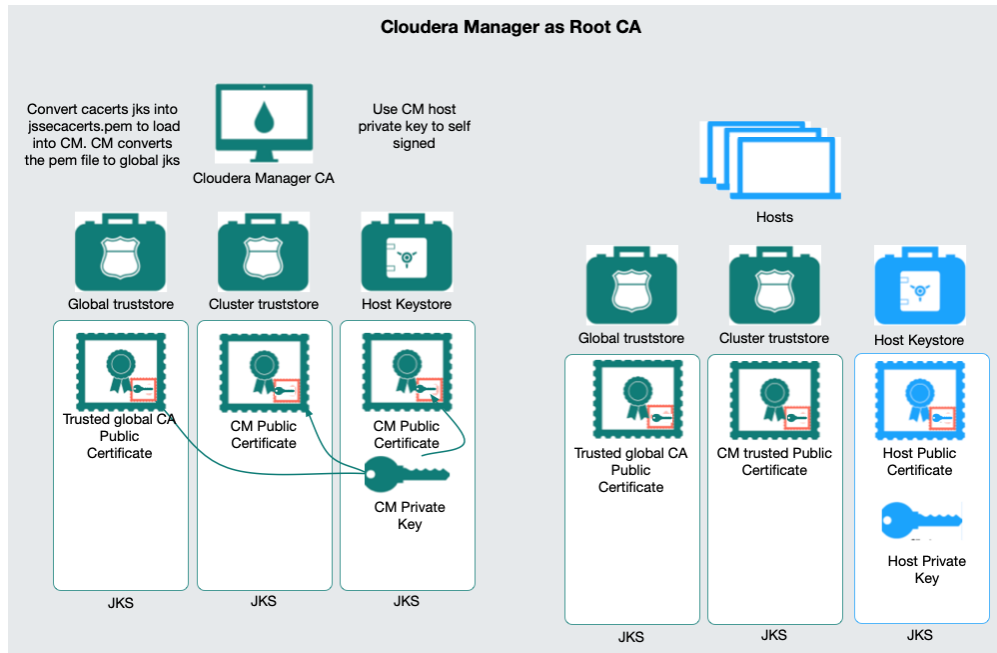
The purpose of this exercise is to verify Auto-TLS and to learn about the underpinnings of Auto-TLS in support of encrypted network traffic. This exercise reviews Auto-TLS configurations while emphasizing the value of Auto-TLS over manual configuration.

Reference Information

The following documents provide information related to this exercise.

- [Encrypting Data in Transit](#)
- [Understanding Keystores and Truststores](#)
- [Choosing manual TLS or Auto-TLS](#)

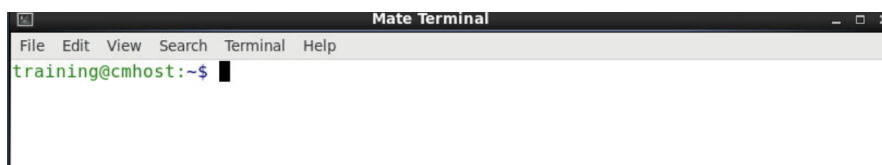
1. Java programs use keystores. Other programs use the pem files. This is why CDP deploys both keystores and pem files.



By default, CDP components communicate across the network in plain text. Auto-TLS distributes the required certificates in the correct formats. These formats include keystore, truststore, and pem files. Auto-TLS places all certificates into `/var/lib/cloudera-scm-agent/agent-certs` on every host. Auto-TLS quickly and easily enables all network traffic for all CDP components to be encrypted.

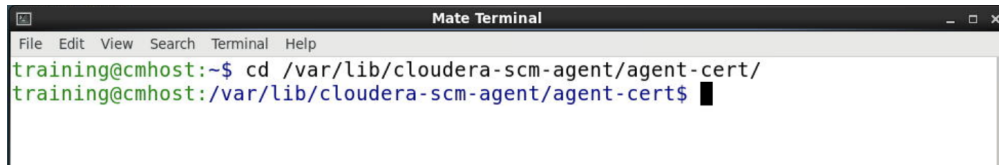
IMPORTANT: Once Auto-TLS is enabled Cloudera Manager will automatically configure all new CDP components with TLS.

2. Open a Mate terminal as the local administrative user, training.



3. Review Auto_TLS certificate files.

3.1 Use the `cd` command to change directory to `/var/lib/cloudera-scm-agent/agent-cert`. A CDP administrator should memorize this directory location.

A screenshot of a terminal window titled "Mate Terminal". The terminal shows a user named "training" at a host named "cmhost". The prompt is "~\$". The user enters the command "cd /var/lib/cloudera-scm-agent/agent-cert/". The prompt changes to "/var/lib/cloudera-scm-agent/agent-cert\$".

```
training@cmhost:~$ cd /var/lib/cloudera-scm-agent/agent-cert/  
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$
```

```
$ cd /var/lib/cloudera-scm-agent/agent-cert
```

3.2 Use the `ls` command to list the keystore files. The `global_truststore.jks` holds all of the trusted CA's. The `cluster_truststore.jks` holds the Cloudera Manager CA. The `host_keystore.jks` is the hosts keystore.

```
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$ ls *jks  
cm-auto-global_truststore.jks  cm-auto-in_cluster_truststore.jks  
cm-auto-host_keystore.jks  
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$
```

```
$ ls *jks
```

3.3 List the directory for the signed public certificates. The `global_cacerts.pem` is from cacerts. The `cluster_ca_cert.pem` is from Cloudera Manager.

```
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$ ls *ca*  
cm-auto-global_cacerts.pem  cm-auto-in_cluster_ca_cert.pem  
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$
```

```
% ls *ca*
```

3.4 The cm-auto-global_cacerts.pem file contains the list of trusted CA's. Page through the file to see the certificates.

```

Mate Terminal
File Edit View Search Terminal Help
Certificate[1]:
Owner: CN=SCM Local CA on cmhost.example.com, ST=CA, C=US
Issuer: CN=SCM Local CA on cmhost.example.com, ST=CA, C=US
Serial number: 4754ee9cd3f37eff
Valid from: Sun Feb 27 13:20:36 PST 2022 until: Fri Feb 26 15:59:59 PST 2027
Certificate fingerprints:
    MD5: 06:60:BD:BF:1E:D3:9F:A0:CB:47:9D:DF:A5:4B:D6:98
    SHA1: 51:49:3C:4A:D0:06:14:21:4E:D7:CB:F0:0E:BB:72:BE:98:E9:77:76
    SHA256: 0B:30:5F:C0:4F:2A:74:17:ED:7D:97:17:32:87:AC:0C:09:C3:B8:81:8D:
A6:7E:15:32:3A:62:33:94:C1:F4:2A
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 3072-bit RSA key
Version: 3

```

```
$ sudo keytool -printcert -file cm-auto-global_cacerts.pem | less
```

3.5 The cm-auto-global_cacerts.pem file contains the Cloudera Manager self-signed certificate. Page through the file to see the certificates.

```

Mate Terminal
File Edit View Search Terminal Help
Certificate[1]:
Owner: CN=SCM Local CA on cmhost.example.com, ST=CA, C=US
Issuer: CN=SCM Local CA on cmhost.example.com, ST=CA, C=US
Serial number: 4754ee9cd3f37eff
Valid from: Sun Feb 27 13:20:36 PST 2022 until: Fri Feb 26 15:59:59 PST 2027
Certificate fingerprints:
    MD5: 06:60:BD:BF:1E:D3:9F:A0:CB:47:9D:DF:A5:4B:D6:98
    SHA1: 51:49:3C:4A:D0:06:14:21:4E:D7:CB:F0:0E:BB:72:BE:98:E9:77:76
    SHA256: 0B:30:5F:C0:4F:2A:74:17:ED:7D:97:17:32:87:AC:0C:09:C3:B8:81:8D:
A6:7E:15:32:3A:62:33:94:C1:F4:2A
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 3072-bit RSA key
Version: 3

```

```
$ sudo keytool -printcert -file cm-auto-global_cacerts.pem | less
```

The Cloudera Manager certificate is first in the file, followed by the public CA certificates. CA:true indicates that Cloudera Manager is a Certificate Authority and Key_CertSign authorizes this certificate to sign other certificates.

3.6 List the directory for the key files. These files contain private keys for the host.

```

training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$ ls *key*pem
cm-auto-host_key_cert_chain.pem  cm-auto-host_key.pem
training@cmhost:/var/lib/cloudera-scm-agent/agent-cert$

```

```
% ls *key*pem
```

4. Login to Cloudera Manager as the administrative user, allan_admin.

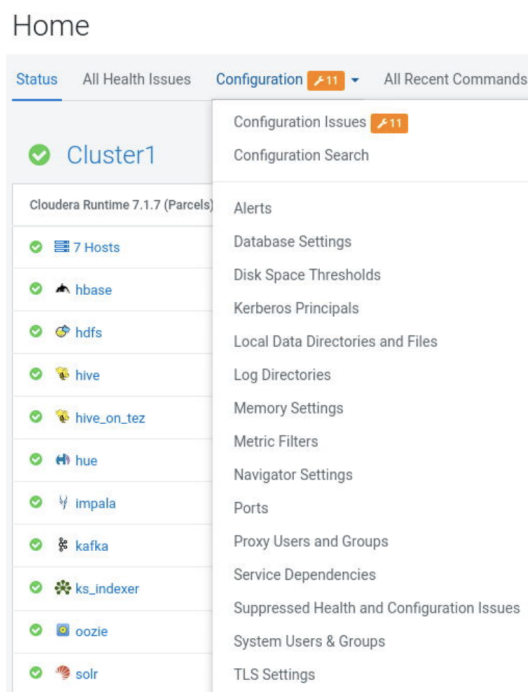
4.1 Login into Cloudera Manager as the administrative user, allan_admin.

☐ Remember me

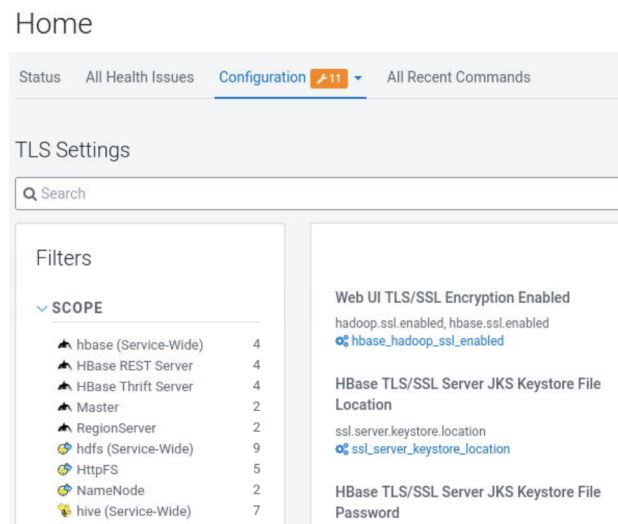
5. Verify properties for encrypting HDFS and YARN network traffic.

5.1 Return to Cloudera Manager Home. In Cloudera Manager there are three ways to view the TLS properties.

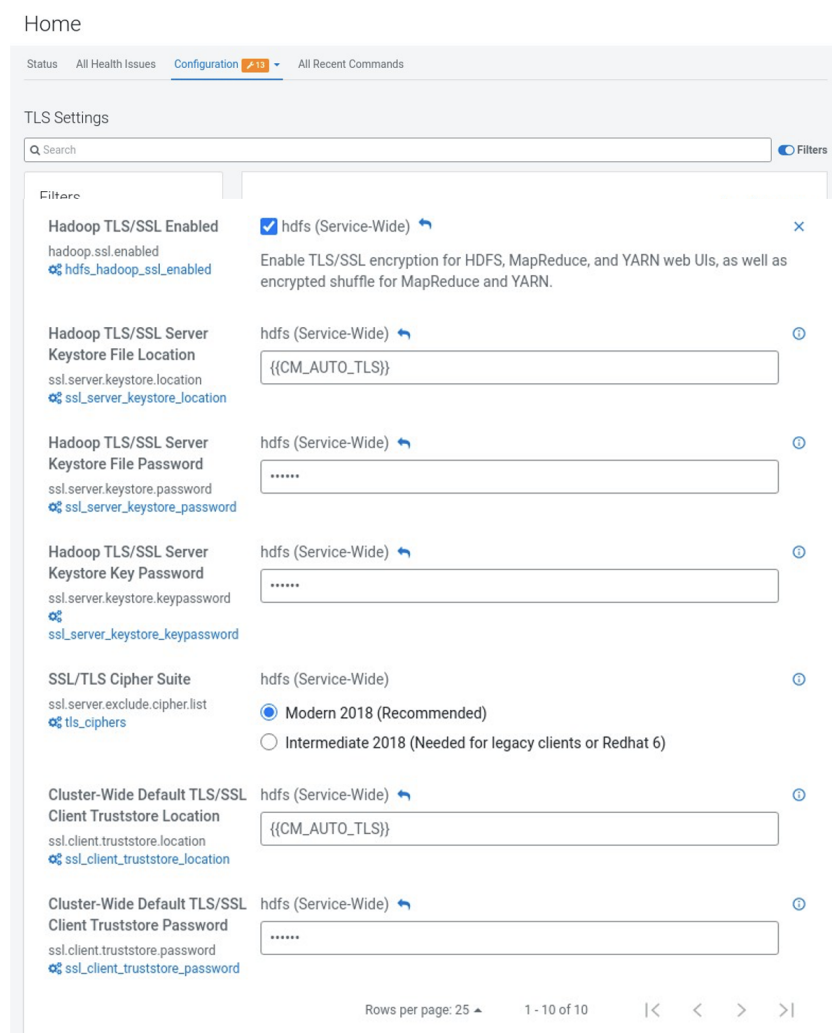
5.2 First, from Cloudera Manager Home, select Configuration, select TLS Settings. Select the filter for NameNode. You can filter for any service.



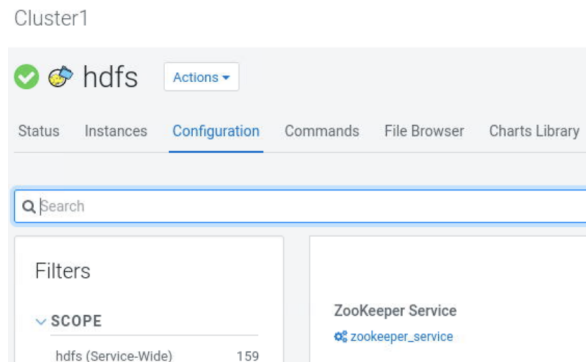
5.3 Second, from Cloudera Manager home select Administration, select Security. On Security select TLS Settings. This will take you to the same listing.



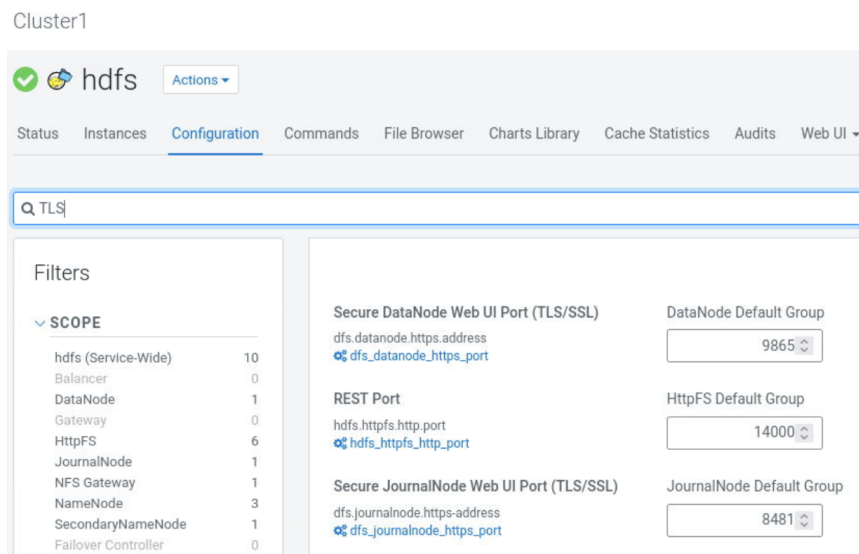
5.4 Select hdfs (Service-Wide) under the Scope heading. Scroll through to review the properties. Find the property for the location of the keystore and truststore.



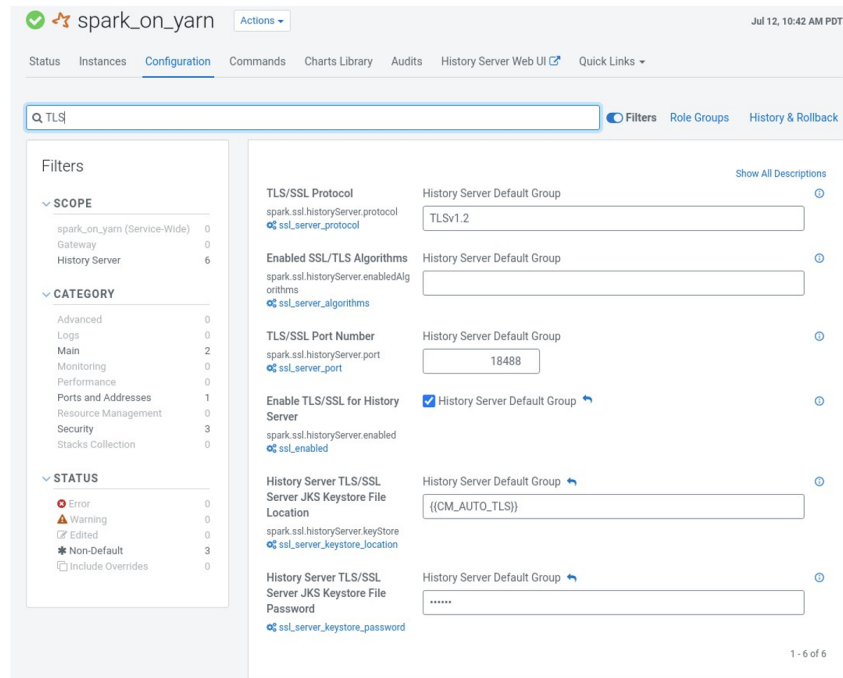
5.5 Third, all the CDP components have their specific configuration for TLS properties. For example, you will find the same properties locating the keystore and truststore. Return to the Cloudera Manager Home page and select hdfs. Select Configuration.



5.6 Search "TLS". Find the properties for locating the keystore and truststore.



5.7 Take time to review other CDP components for TLS configurations, such as Spark, HBase, Solr, Hive, or Impala. Compare and contrast TLS configuration properties. You will find many are similar but they are not all identical.



6. The steps for configuring TLS manually follow the same logic. If you use the manual installation method, you must account for each unique configuration. By using Auto-TLS you greatly simplify the deployment of TLS. Additionally, Auto-TLS can be used to quickly roll certificates when updates are required. Return to the Cloudera Manager Home.