mod16_ex02: Deploying Auto-TLS

The purpose of this exercise is to configure HTTPS for all CDP components using Auto-TLS. Auto-TLS is an automation tool for easily deploying and rolling certificates to every host in a CDP cluster. This exercise depends upon completion of the Hands-On Exercise Creating the jssecacerts File.

Cloudera Manager will use a self-signed certificate to become the root Certificate Authority. This configuration is recommended for proof of concepts, training, development, and troubleshooting environments. It is not recommended for staging or production.

Cloudera Manager will use the Auto-TLS wizard to distribute and roll certificates across a CDP cluster. Auto-TLS will load the jsscaccerts.pem file, create the required X509 formats certificates, and distribute these to every host in the cluster. The certificates are stored in /var/lib/cloudera-scm-agent/agent-cert. The Cloudera Manager server service, Cloudera Management Service, and the CDP Runtime must be restarted to complete the process.

Reference Information

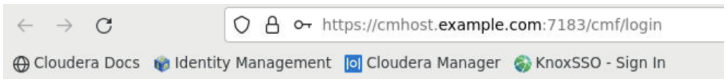
The following documents provide information related to this exercise.

Use Cloudera Manager to generate internal CA and corresponding certificates

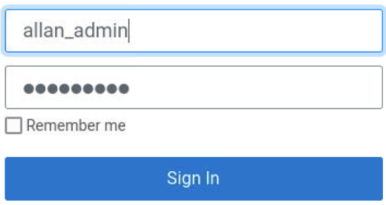
Converting file encodings for TLS/SSL certificates and keys

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

1.1 On the Firefox browser bookmark toolbar select Cloudera Manager.

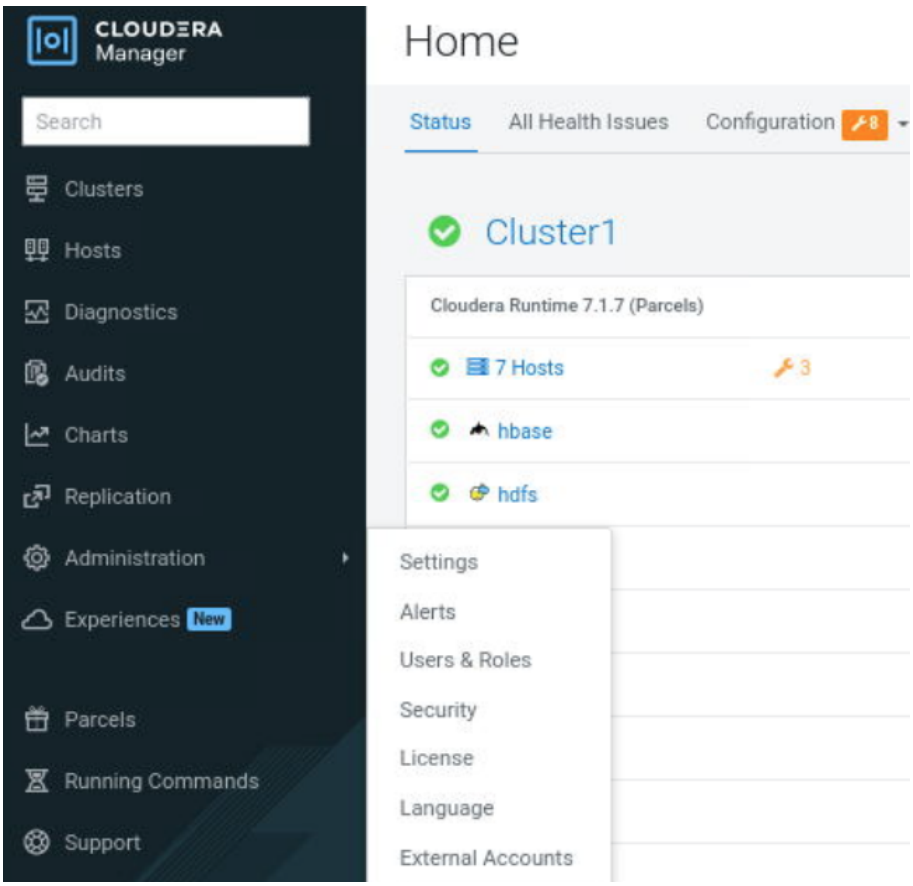


1.2 Login as the user allan_admin with password <password>.

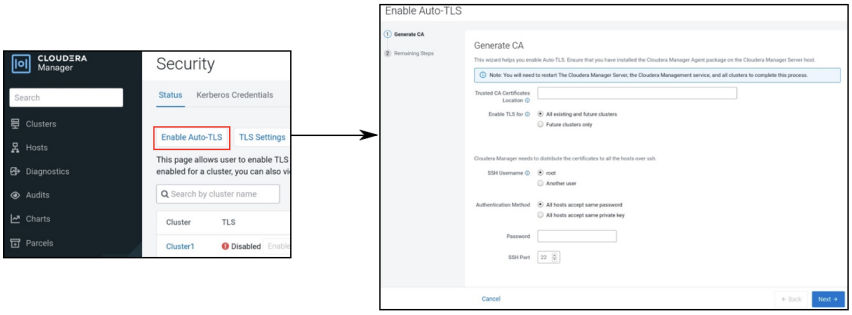


2. Deploy Auto-TLS.

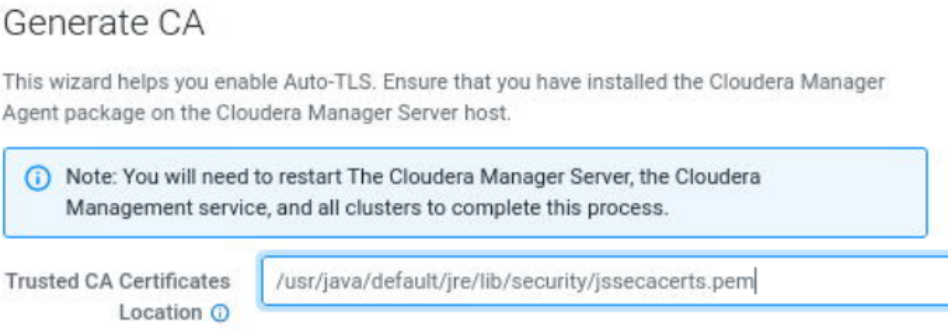
2.1 Select Administration > Security.



2.2 On the Status tab Select Enable Auto-TLS.

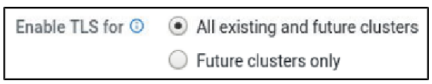


2.3 In Trusted CA Certificates Location enter "/usr/java/default/jre/lib/security/jssecacerts.pem".

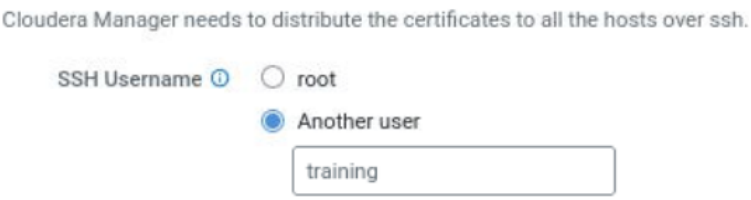



```
/usr/java/default/jre/lib/security/jssecacerts.pem
```

2.4 Select the option All existing and future clusters.

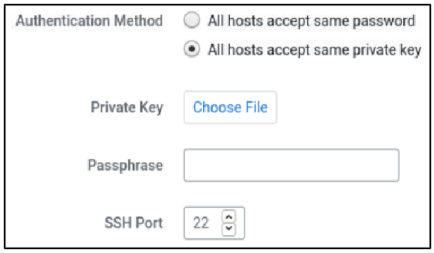


2.5 Select the option Another user. Enter the user training.



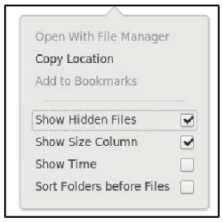
The CDP admin user training is configured with sudo with no password and has the private key and public certificate granting ssh access with no password. The CDP admin user allan_admin is not configured with these Linux privileges.

2.6 Select the option All hosts accept same private key.

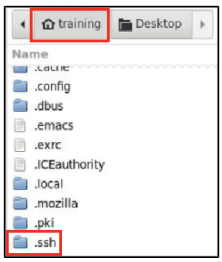


2.7 Select Choose File to select a private key.

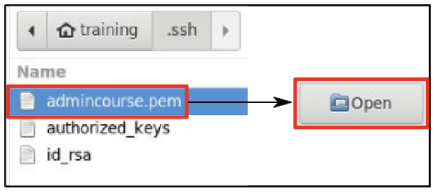
2.8 Right click on the File Upload screen and select Show Hidden files.



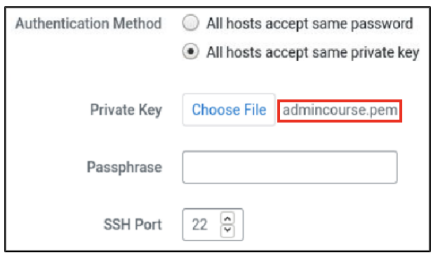
2.9 Click on the training directory. Double-click the .ssh folder.



2.10 Select admincourse.pem. Click Open.

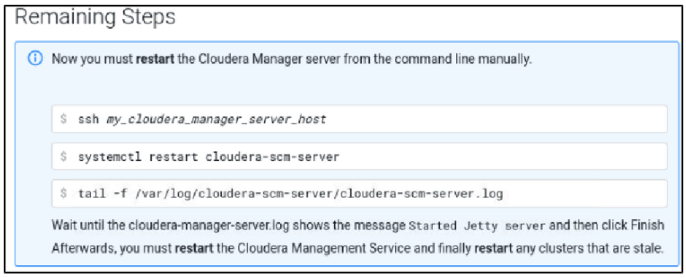


2.11 Verify the admincourse.pem filename appears on the page. Leave Passphrase blank. Leave SSH Port at 22.



2.12 Click Next. Auto-TLS will take a few minutes to install the keystores, keys, and certificates.

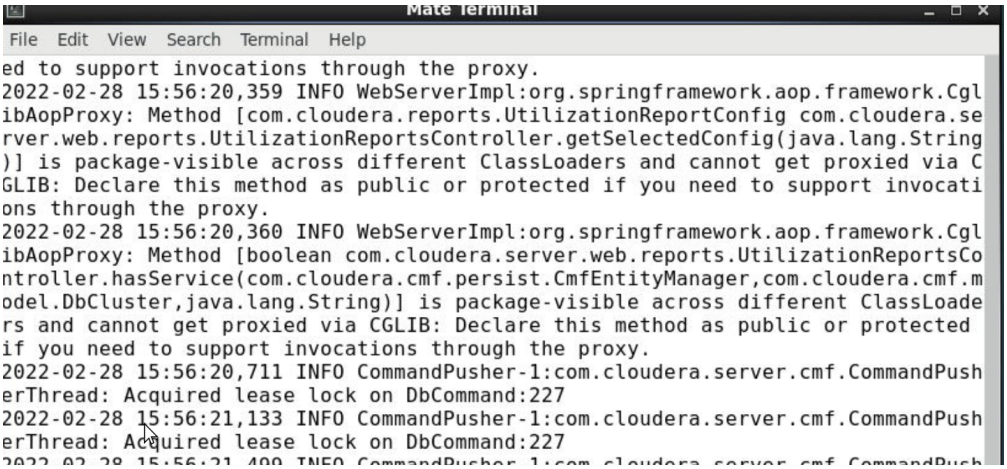
2.13 The remaining steps are displayed. You must read this carefully.



2.14 Open a Mate terminal. Use the sudo and systemctl commands to restart the cloudera-scm-server.


```
$ sudo systemctl restart cloudera-scm-server
```

2.15 The restart will run for up to 2 minutes. Ensure the restart is finished by checking for the startup of the WebServer. Open a second Mate Terminal. You may tail cloudera-scm-server.log or you can check with grep for WebServerImpl. Check the datetime stamp for a current restart.

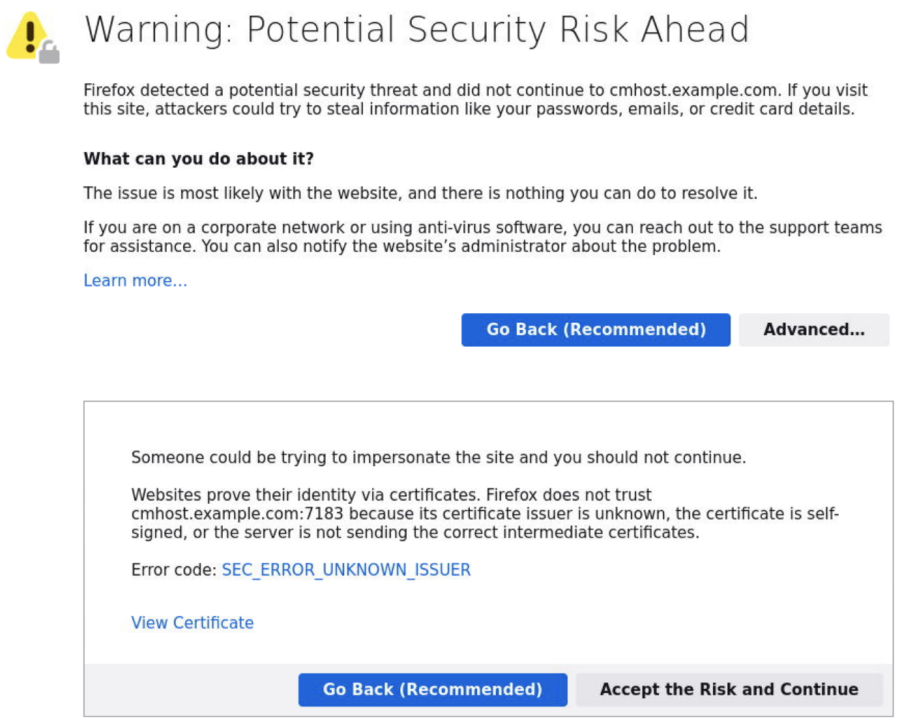



```
$ sudo tail -f /var/log/cloudera-scm-server/cloudera-scm-server.log
```

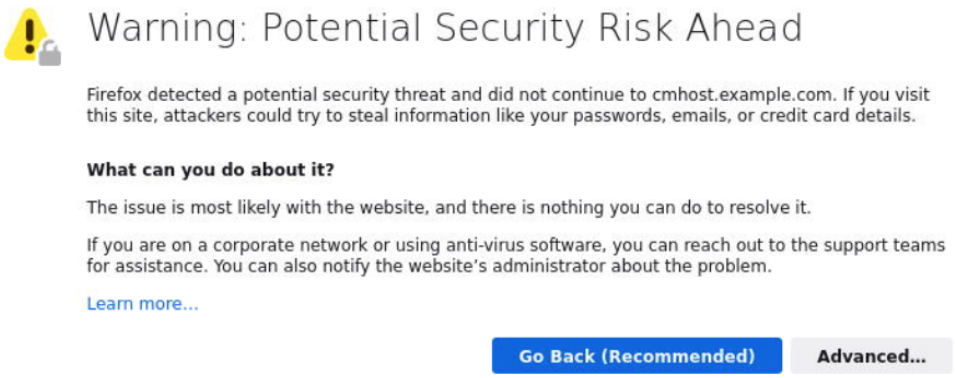
2.16 When "Started Jetty server" appears, on Cloudera Manager click Finish.

3. Setup the Firefox Browser. Encrypted network connections, HTTPS, requires browsers to import the public certificate.

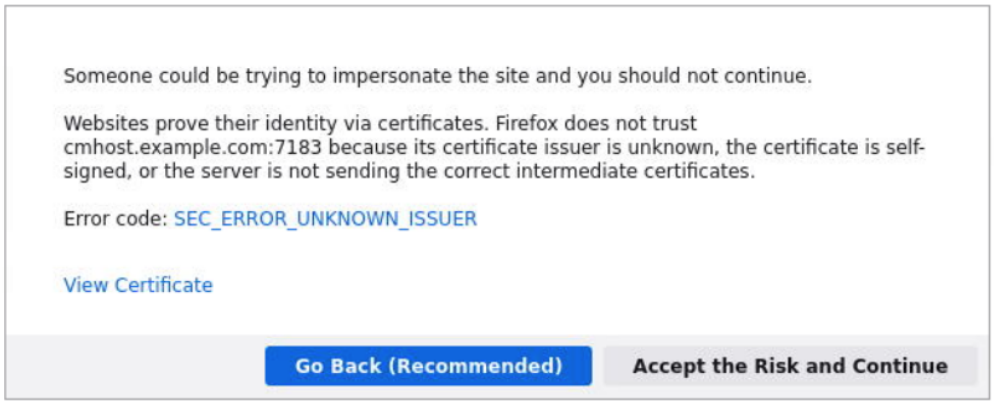
3.1 You will get a Firefox warning about the Security Risk.



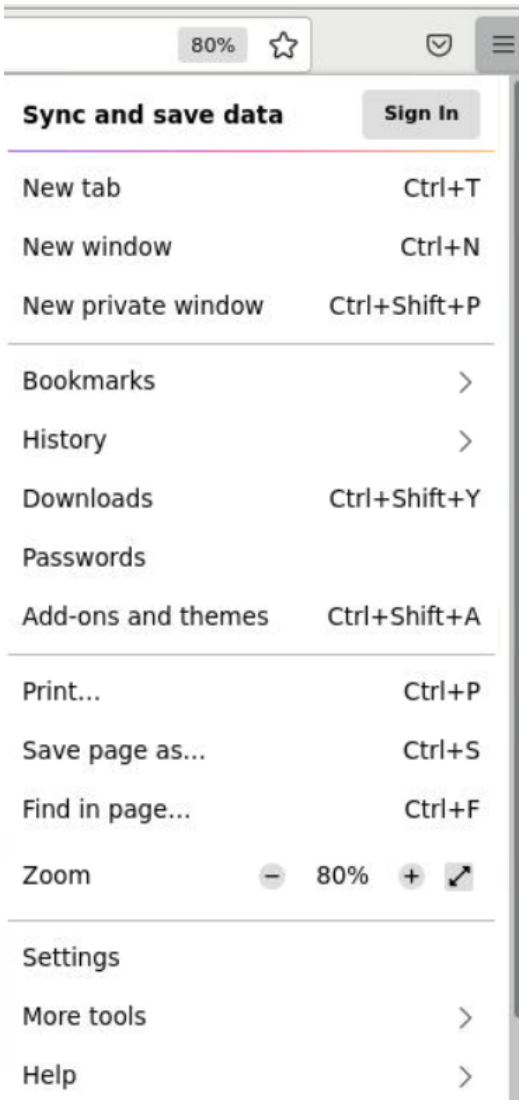
3.2 Select Advance. If needed enter the https URL for cmhost (https://cmhost.example.com:7183).



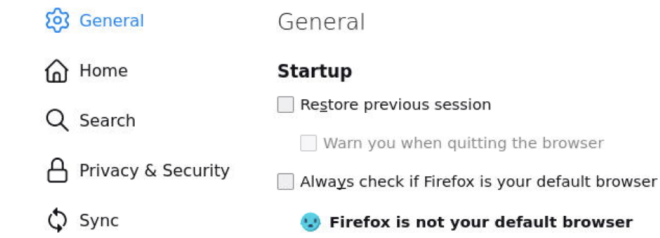
3.3 Select Accept the Risk and Continue. A warning about impersonation is displayed. The reason for lack of trust is the use of a self-signed certificate.



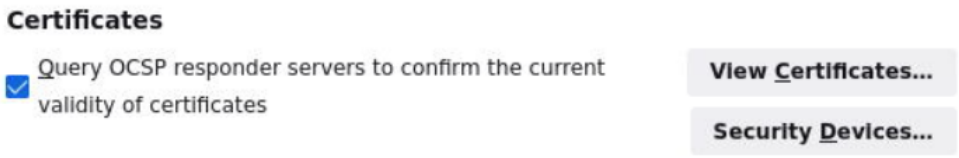
3.4 From the Firefox action menu select Settings.



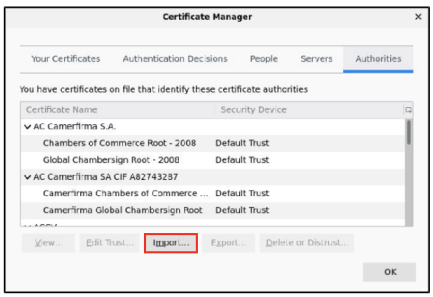
3.5 On the left hand side menu select Privacy & Security.



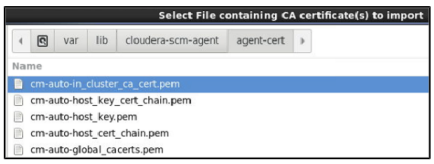
3.6 Scroll down the page. In Certificates select View Certificates.



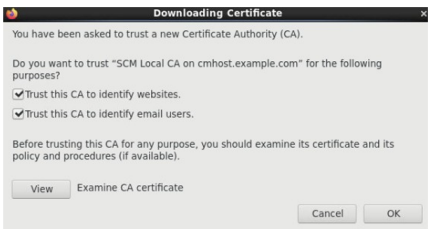
3.7 Select Import.



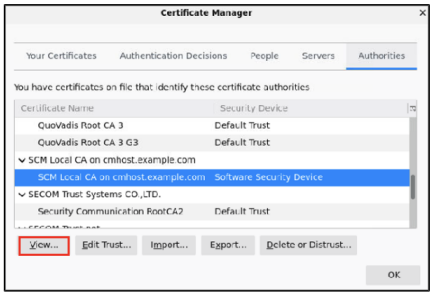
3.8 Navigate to /var/lib/cloudera-scm-agent/agent-cert, select cm-auto-in_cluster_ca_cert.pem, and click Open. This file is the self-signed public certificate.



3.9 Select the checkboxes for Trust this CA to identify websites and Trust this CA to identify email users. Click OK.

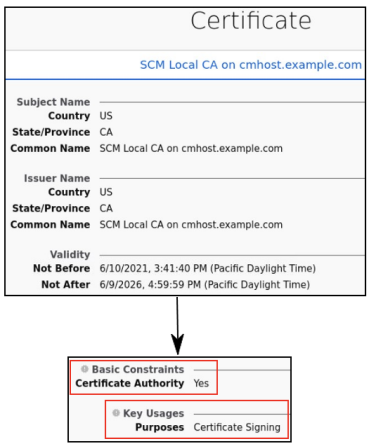


3.10 In Certificate Manager, scroll down to the certificate name SCM Local CA on cmhost.example.com with Security Device of Software Security Device and select the entry. This is the Cloudera Manager self-signed certificate. Click View to view certificate details.

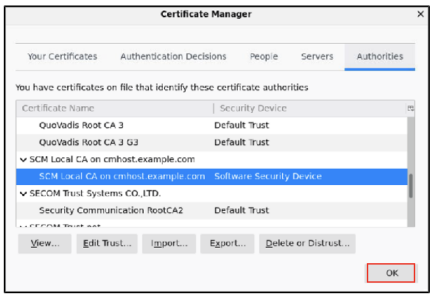


NOTICE You may have to exit the Certifcate Manager view and reopen it.

3.11 Exit the Certificate Manager window. Select View Certificate. Scroll down to select SCM Local CA on cmhost.example.com. Select View to validate the Certificate Authority is used for Certificate Signing.



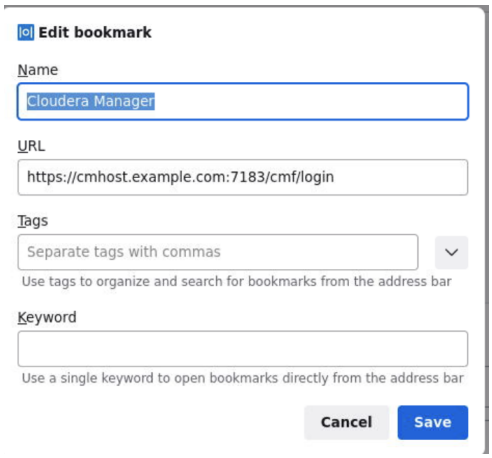
3.12 Return to the Preferences tab to see Certificate Manager. Click OK.



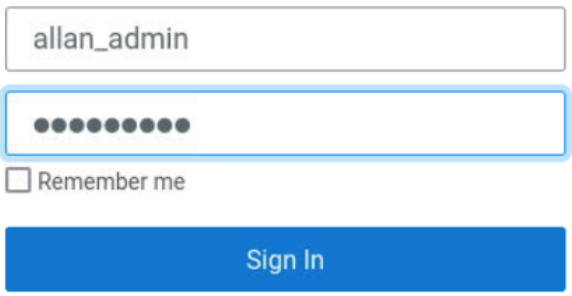
3.13 Click x Close on the Settings and View tab.

4. Restart Cloudera Manager and the Cluster. Login to a Secure Cloudera Manager. The Cloudera Management Service and the CDP Runtime must be restarted. Client configurations must be deployed. This section will take approximately 20 to 30 mins.

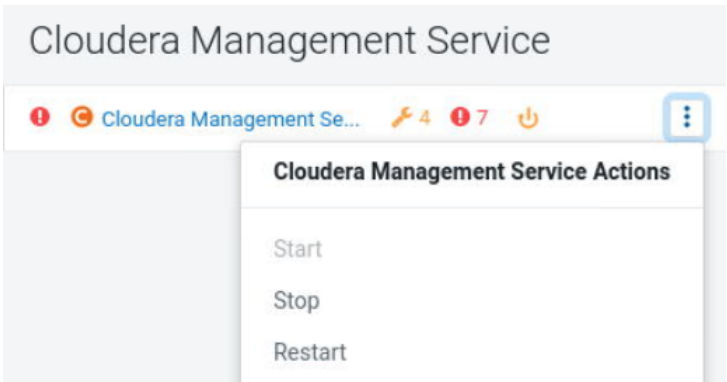
4.1 Select the Cloudera Manager Firebox bookmark. Right click to edit the book mark. Edit the URL to https://cmhost.example.com:7183. Click Save. Select Cloudera Manager.



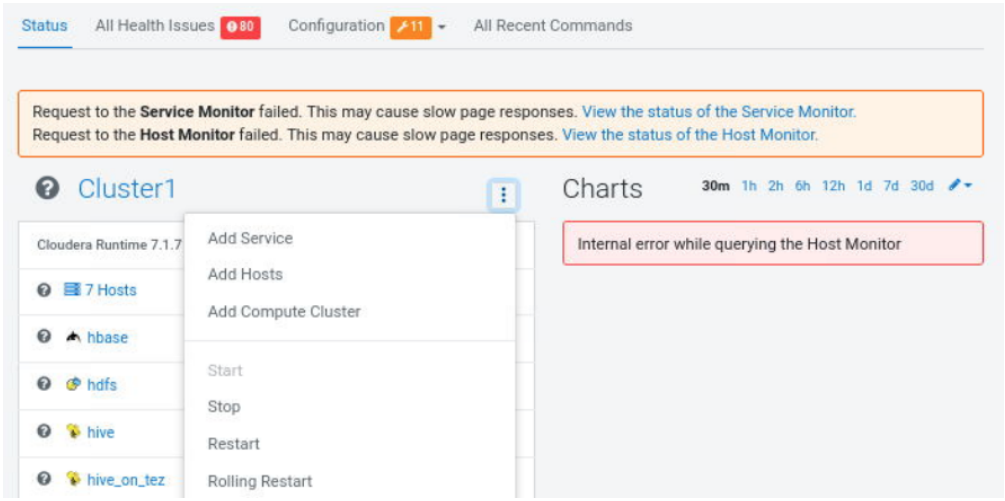
4.2 Log into Cloudera Manager as the administrative user, allan_admin, with password <password>.



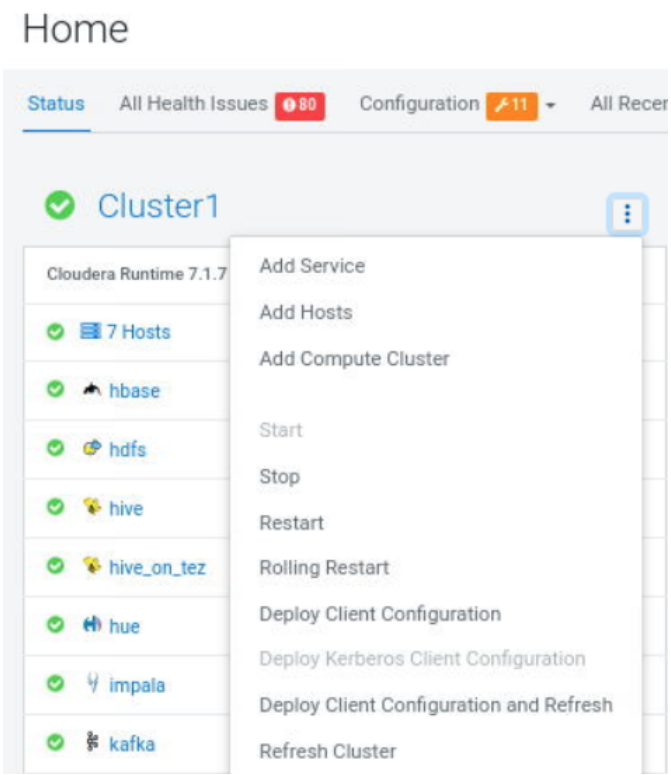
4.3 On Cloudera Manager Home scroll down to Cloudera Management Service. Select action. Select Restart. This takes up to 4 to 7 mins. Wait until Finished.



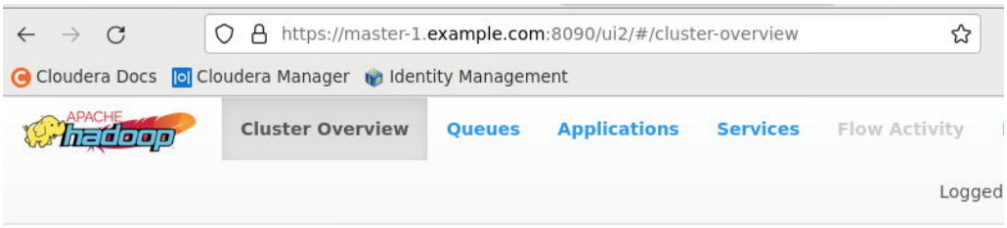
4.4 Upon successful restart of Cloudera Manager Service, select Cluster action. Select Restart. This will take up to 7 to 10 mins.



4.5 Upon successful restart of CDP Runtime, select Cluster action select Deploy Client Configuration and Refresh. This will take up to 5 mins.



4.6 Upon successful deployment of client configurations select YARN. Select Web UI > ResourceManager Web UI. Validate it opens with https.



4.7 Close the YARN tab.

5. Return to the Cloudera Manager Home.

TLS https is now enabled throughout the CDP cluster.