THALES

Cloudera Data Platform: Integration Guide

THALES LUNA HSM

Document Information

Document Part Number	007-000730-001
Revision	B
Release Date	5 November 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

Cloudera Data Platform (CDP) combines Hortonworks and Cloudera technologies to deliver industry's first enterprise data cloud. CDP delivers powerful self-service analytics across hybrid and multi-cloud environments, along with sophisticated and granular security and governance policies that IT and data leaders demand. It was initially delivered as a public cloud service and followed up with Data Center, a comprehensive data management and analytics platform for on-premises IT environments. Cloudera Manager is a component of Cloudera Data Platform (CDP) that can be used to manage, configure, and monitor CDP Data Center clusters and Cloudera Runtime services.

This integration describes how to use Cloudera Manager for configuring Ranger KMS and Key Trustee Server that secure the Data at Rest Encryption Keys on Thales Luna HSM. The benefits of securing the cryptographic keys with a Thales Luna HSM include:

- Secure generation, storage and protection of keys on FIPS 140-2 level 3 validated hardware
- Full life cycle management of the keys
- Access to the HSM secure audit trail

Certified Platforms

Certified platforms for Luna HSM

The following platforms are certified with Luna HSM:

Platform Certified	Cloudera Manager	Cloudera Runtime	HSM Type	HSM Client
Red Hat Enterprise Linux 7 (64 bit)	7.5.1	7.1.6	Luna s/w v7.7.0 Luna f/w 7.7.1	UC-10.3.0 UC-10.4.0
Cent OS 7 (64 bit)	7.1.1	7.1.0	Luna s/w v7.4.0 Luna f/w 7.4.0	UC-10.2.0

NOTE: CDP Integration is tested in HA as well as FIPS mode.

NOTE: CDP Integration using Ranger KMS with Key Trustee Server is not supported in FIPS mode from Luna f/w 7.7.0 onwards.

NOTE: CDP Integration with Luna f/w 7.7.0 onwards supported in FIPS only with Ranger KMS when UC v10.4.0 is used.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Prerequisites

Before you begin the integration, ensure you have completed the following tasks:

Configure Thales Luna HSM

To configure Luna HSM.

1. Ensure that the HSM is set up, initialized, provisioned, and ready for deployment. Refer to Luna HSM documentation for help
2. Create a partition that will be later used by Cloudera Service.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
# /usr/safenet/lunaclient/bin/lunacm
   lunacm (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights
   reserved.
   Available HSMs:
   Slot Id ->              0
   Label ->                Cloudera01
   Serial Number ->        1238696044938
   Model ->                LunaSA 7.4.0
   Firmware Version ->     7.4.0
   Configuration ->        Luna User Partition With SO (PW) Key Export With
   Cloning Mode
   Slot Description ->     Net Token Slot
   FM HW Status ->         Non-FM

   Current Slot Id: 0
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Controlling User Access to the HSM

> **NOTE:** This section is applicable only for Linux users.

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM by adding them to the **hsmusers** group. The client software installation automatically creates the **hsmusers** group. The **hsmusers** group is retained when you uninstall the client software, allowing you to upgrade the software while retaining your **hsmusers** group configuration.

Adding a user to hsmusers group

To allow non-root users or applications access to the HSM, assign the users to the **hsmusers** group. The users you assign to the **hsmusers** group must exist on the client workstation.

1. Ensure that you have **sudo** privileges on the client workstation.
2. Add a user to the hsmusers group.

   ```
   # sudo gpasswd --add <username> hsmusers
   ```

   Where `<username>` is the name of the user you want to add to the hsmusers group.

Removing a user from hsmusers group

1. Ensure that you have sudo privileges on the client workstation.
2. Remove a user from the hsmusers group.

   ```
   # sudo gpasswd -d <username> hsmusers
   ```

   Where `<username>` is the name of the user you want to remove from the **hsmusers** group. To view the change, you need to log in again.

   > **NOTE:** The user you delete will continue to have access to the HSM until you reboot the client workstation.

Set up Cloudera Data Platform

Cloudera recommends using Cloudera Manager to deploy the Cloudera Data Platform Services. Cloudera Manager is a component of Cloudera Data Platform (CDP). Cloudera Manager is an application you use to manage, configure, and monitor CDP Data Center clusters and Cloudera Runtime services.

The Cloudera Manager server runs on a host in your CDP Data Center deployment and manages your clusters using Cloudera Manager Agents that run on each host in the cluster. The Cloudera Manager Admin Console is a web application that administrators and others can use to manage CDP Data Center deployments. Using the Cloudera Manager Admin Console, you can start and stop the cluster and individual services, add new services, manage security, and upgrade the cluster.

Refer to *Cloudera Manager Documentation* before you begin a production installation of Cloudera Manager, Cloudera Runtime, and other managed services. You should also review the Cloudera Data Platform Requirements and Supported Versions, in addition to the Cloudera Data Platform Release Notes.

> **NOTE:** To browse to the Cloudera Documentation for detailed information, refer to
>
> https://docs.cloudera.com/cloudera-manager/

Cloudera Data Platform provides two types of KMS services:

- **Ranger KMS**: This option stores only the master key in Luna partition and encryption zone keys are stored encrypted in the database.
- **Ranger KMS with Key Trustee Server**: This stores all encryption zone keys in Luna partition.

Configuring Ranger KMS using Thales Luna HSM

This section demonstrates how to initialize the Ranger KMS that uses Thales Luna HSM to generate the Ranger KSM DB Master Key that protects the encryption zone keys stored in DB. It is assumed that you have installed and configured the Cloudera Manager and have set up a cluster with the required services. Luna Client is installed and configured on the host where you have installed or planning to install the Ranger KMS. To configure Ranger KMS for using Thales Luna HSM:

1. Copy the LunaProvider.jar and libLunaAPI.so from <LunaClientInstallationPath>/jsp/lib folder to <JavaInstallationPath>/jre/lib/ext folder.

   ```
   # cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /usr/lib/jvm/java-
      1.8.0-openjdk-1.8.0.252.b09-2.el7_8.x86_64/jre/lib/ext/
   ```

   ```
   # cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /usr/lib/jvm/java-1.8.0-
      openjdk-1.8.0.252.b09-2.el7_8.x86_64/jre/lib/ext/
   ```

2. Add LunaProvider in the java.security file available at <JavaInstallationPath>/jre/lib/security/ folder.

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=sun.security.rsa.SunRsaSign
   security.provider.3=sun.security.ec.SunEC
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   security.provider.5=com.sun.crypto.provider.SunJCE
   security.provider.6=com.safenetinc.luna.provider.LunaProvider
   security.provider.7=sun.security.jgss.SunProvider
   security.provider.8=com.sun.security.sasl.Provider
   security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
   security.provider.10=sun.security.smartcardio.SunPCSC
   ```

3. Make secret keys extractable. Add the following to the java.security file at the end of the provider list.

   ```
   com.safenetinc.luna.provider.createExtractableKeys=true
   ```

4. Open a web browser and go to http://<server_host>:7180, where <server_host> is the FQDN or IP address of the host that's running Cloudera Manager Server.

   > **NOTE:** If you enabled auto-TLS, you are redirected to https://<server_host>:7183, and a security warning is displayed. You may need to indicate that you trust the certificate, or may have to click to proceed to the Cloudera Manager Server host.

5. Log in to Cloudera Manager Admin console. The default credentials are:

   Username: `admin`

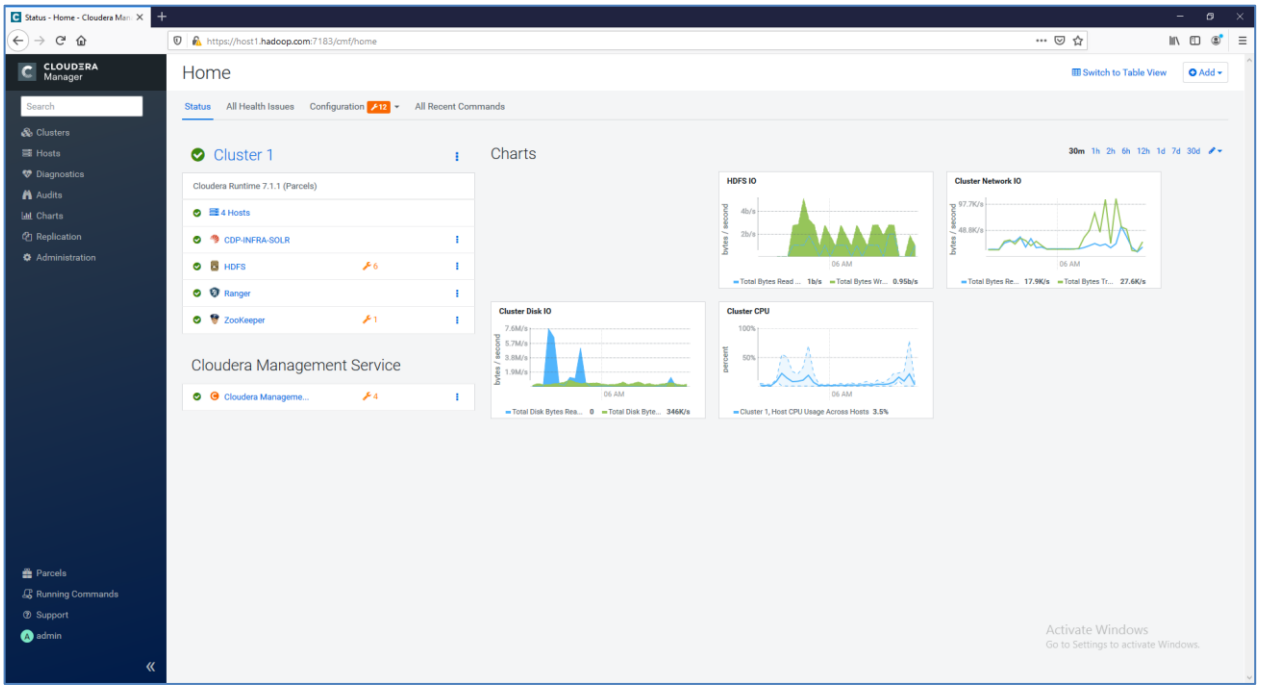
   Password: `admin`

   > **NOTE:** You can change the password using Cloudera Manager after you run the installation wizard. Although Cloudera Manager does not support changing the `admin`

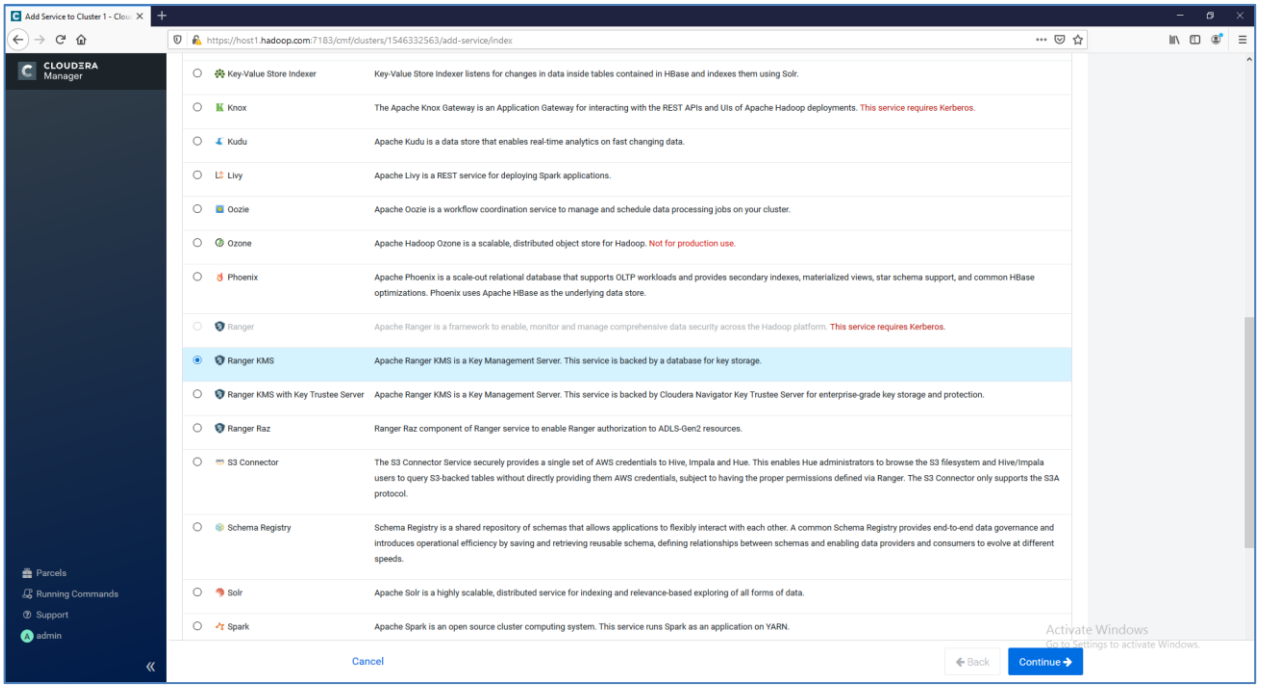
username for the installed account, you can add a new user, assign administrative privileges to the new user, and then delete the default `admin` account.

NOTE: Skip steps 6-16, if Ranger KMS Service is already installed and running.

6. On the cluster **Home** page, click the More Options icon (⋯) and then click **Add Service**.

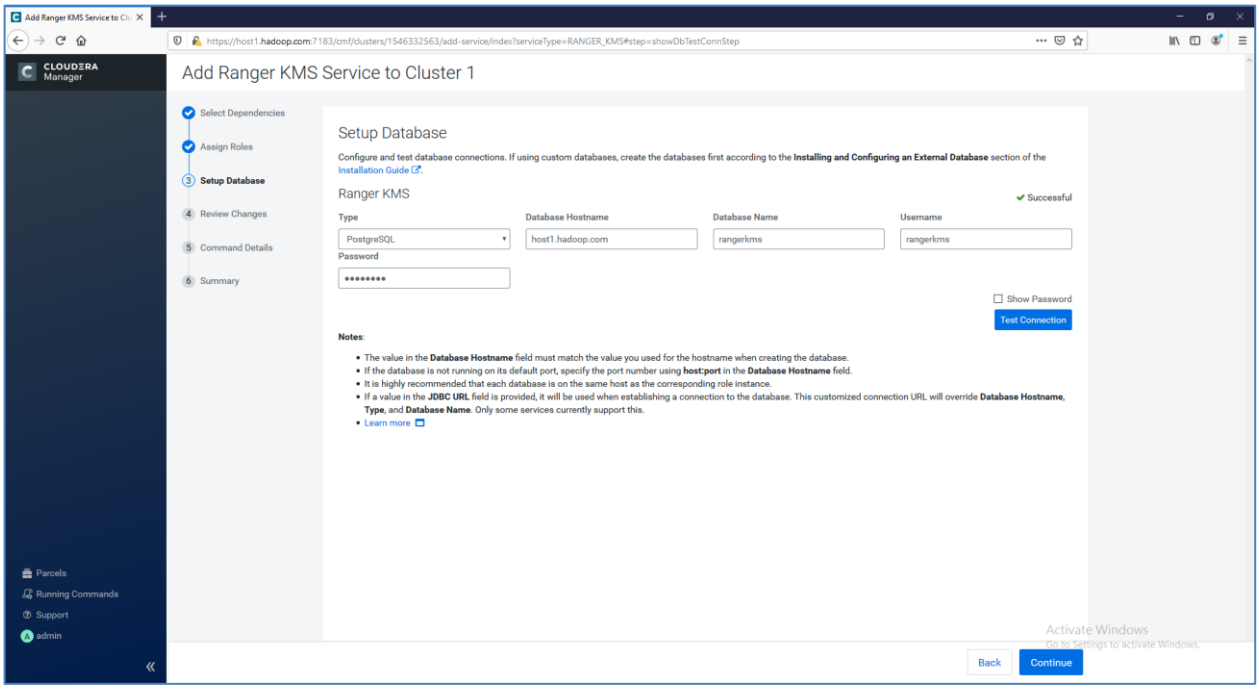


7. Select **Ranger KMS** and click **Continue**.

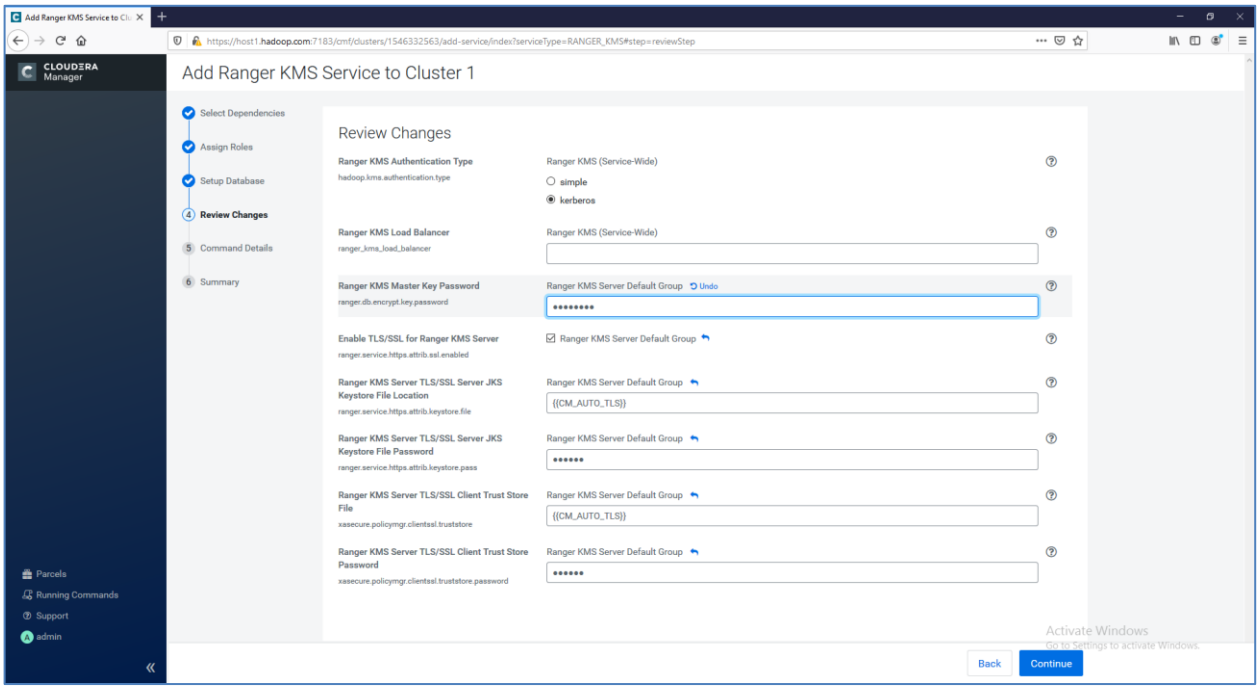


8. A wizard will open to Add Ranger KMS Service to Cluster. Follow the wizard to install Ranger KMS.

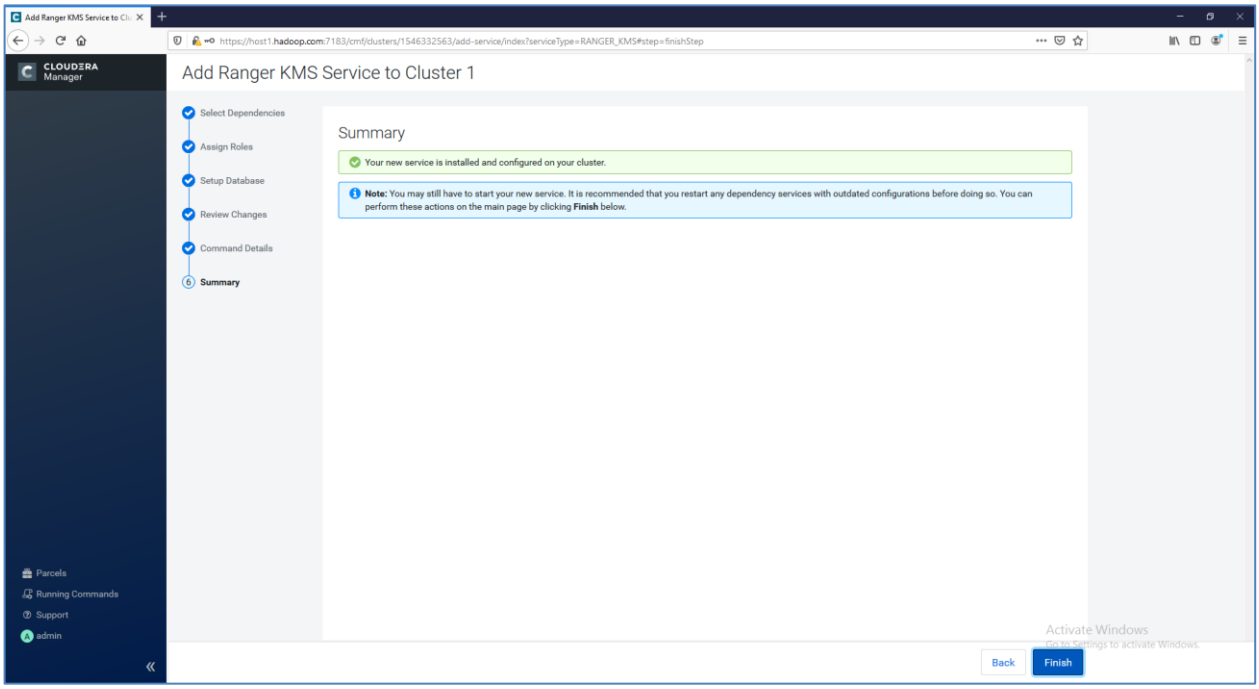
9. On the **Assign Roles** page, select the host on which Luna Client is installed and click **Continue**.
10. On **Setup Database** page, provide the database details for Ranger KMS and click **Test Connection**. Click **Continue** to proceed after you see the message “Successful” on the page.



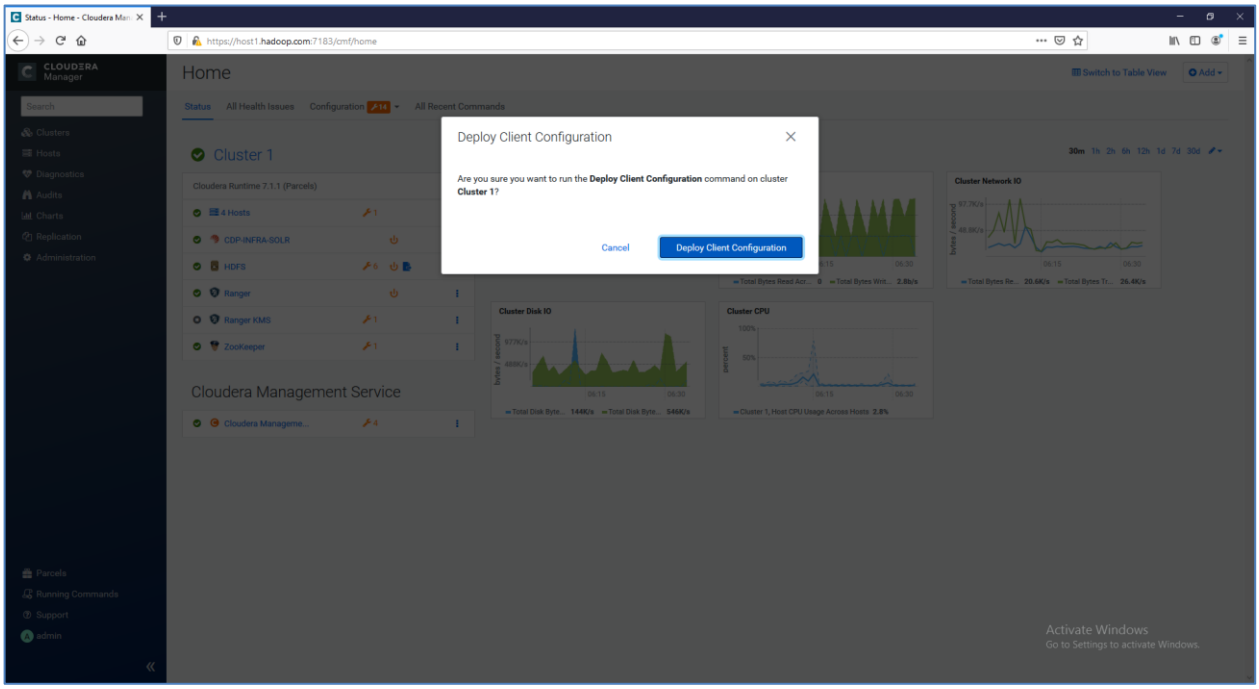
11. On **Review Changes** page, provide **Ranger KMS Master Key Password** and click **Continue**.



12. Wait for the command to finish that will install the Ranger KMS service. After the service is installed successfully, click **Continue** and then **Finish**.

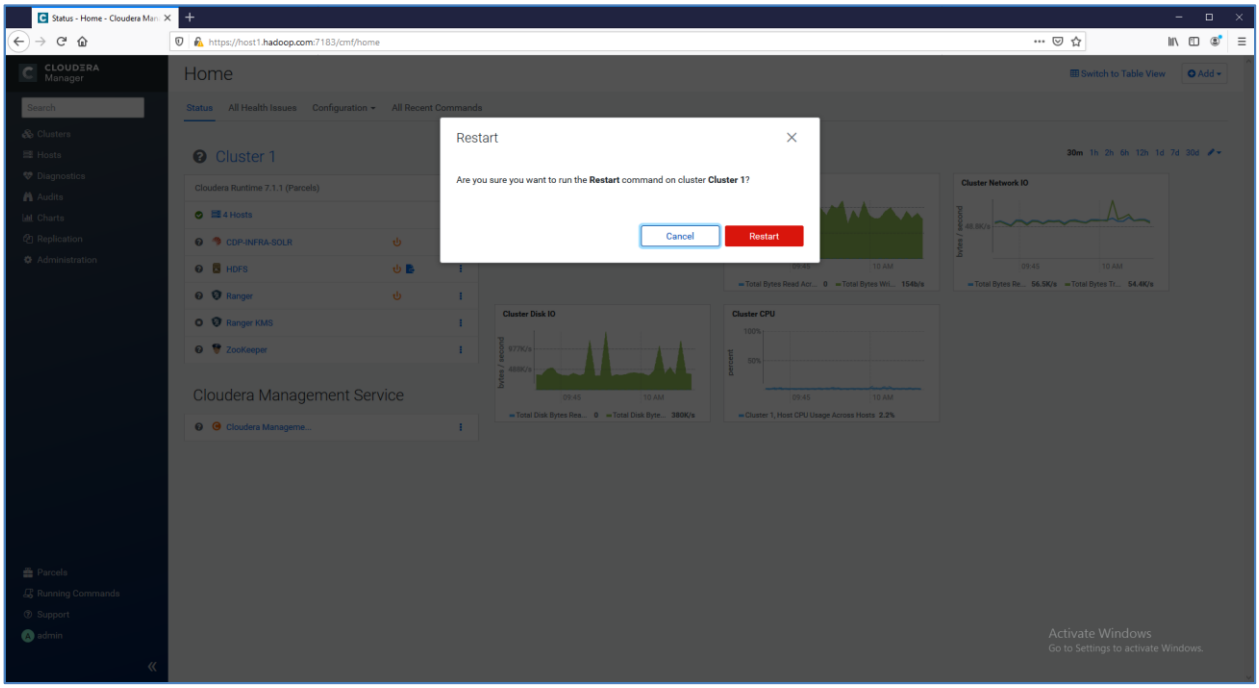


13. On the cluster **Home** page, click the More Options icon (⋯) and then click **Deploy Client Configuration**. Click the **Deploy Client Configuration** again when the confirmation window pops up.

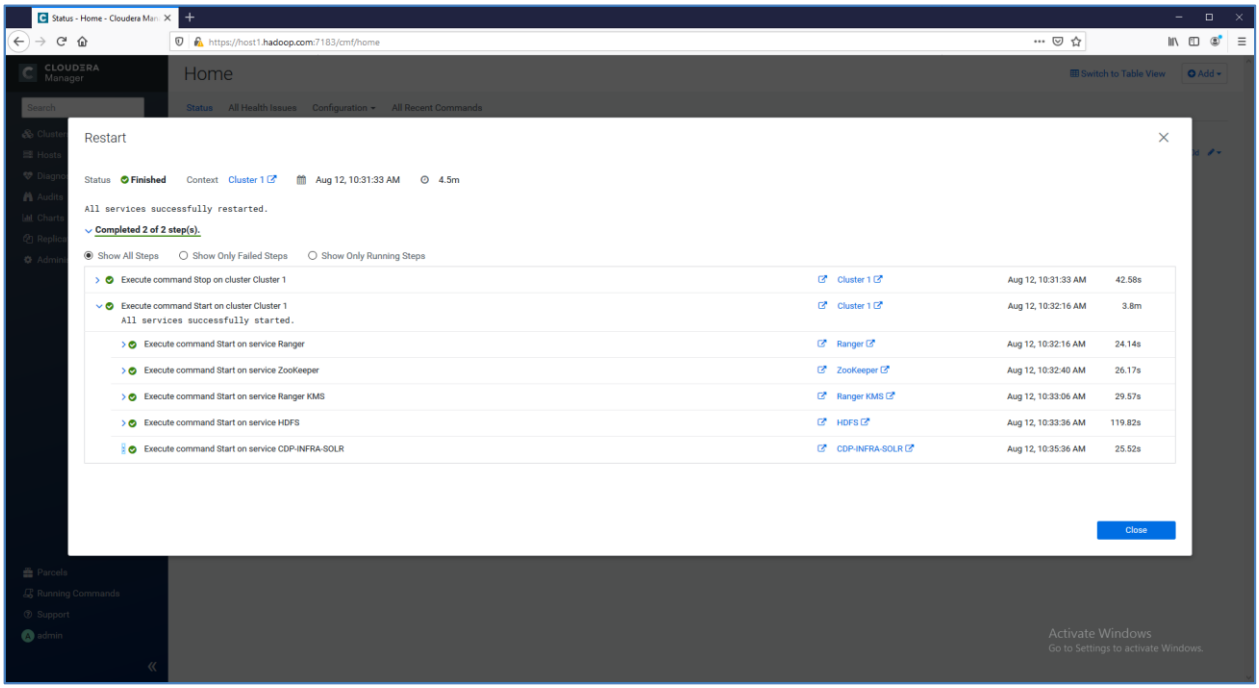


14. Click **Close** when successfully deployed all client configurations.

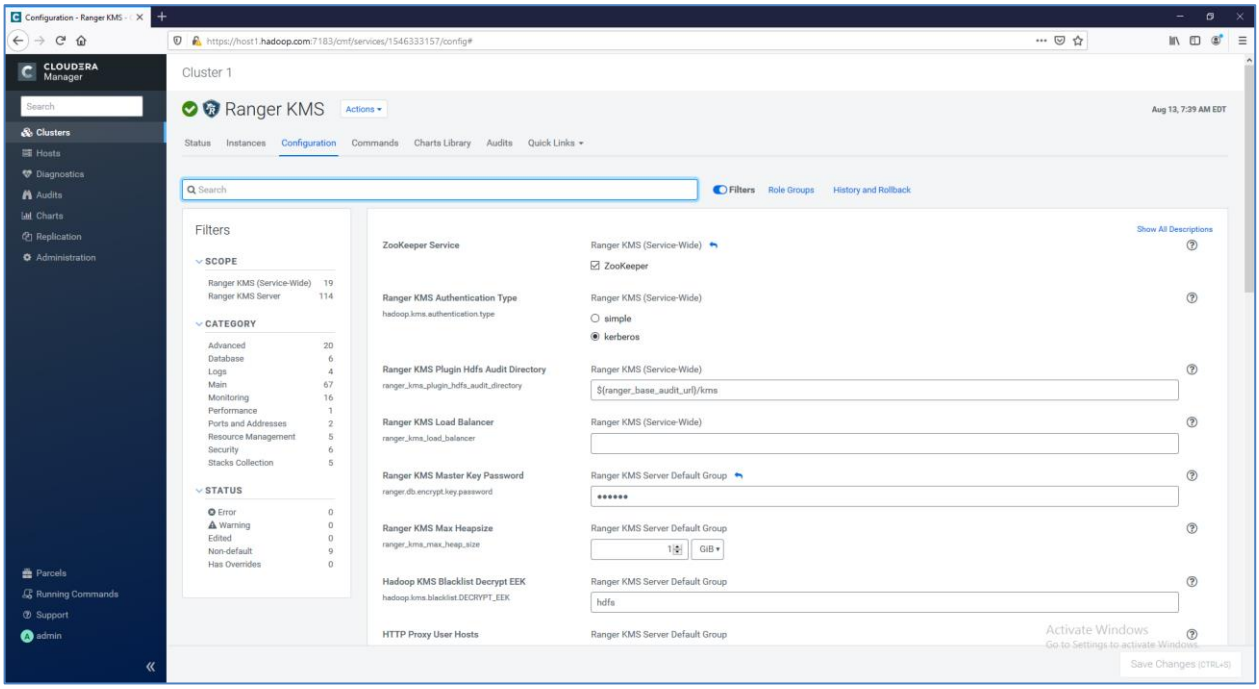
15. On the cluster **Home** page, click the More Options icon (⋯) and then click **Restart**. Click the **Restart** again when the confirmation window pops up.



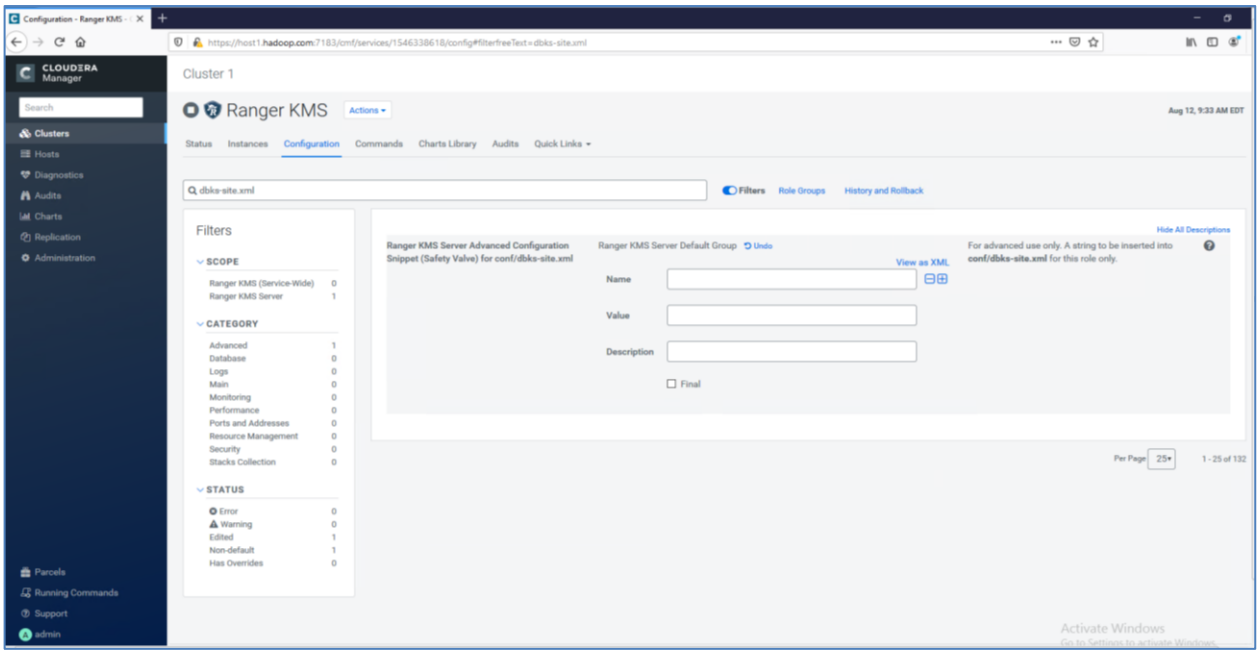
16. Click **Close** when all the services have started successfully.



17. On Cluster Home, click **Ranger KMS** and then **Configuration**.



18. On the **Ranger KMS** configuration page, type `dbks-site.xml` in the **Search** bar. Click **[+]** to expand the **Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml.**



19. You will see the **Name**, **Value** and **Description** fields. Click **[+]** icon to add more values. In the Name, Value and Description text boxes, enter the following information to enable Luna HSM:

    Name: `ranger.ks.hsm.enabled`

    Value: `true`

    Description: `Enable HSM Encryption`

Name: `ranger.ks.hsm.type`

Value: `LunaProvider`

Description: `Luna HSM Type`

Name: `ranger.ks.hsm.partition.name`

Value: `ClouderaHA`

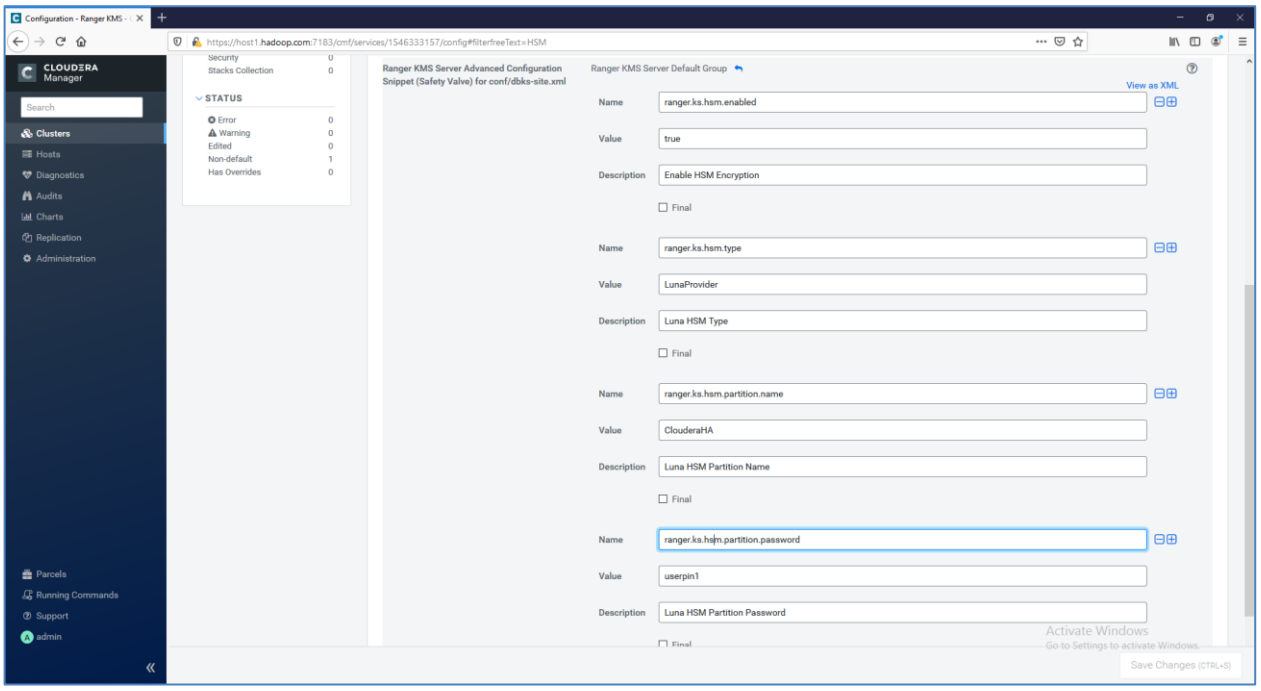
Description: `Luna HSM Partition Name`

Name: `ranger.ks.hsm.partition.password`

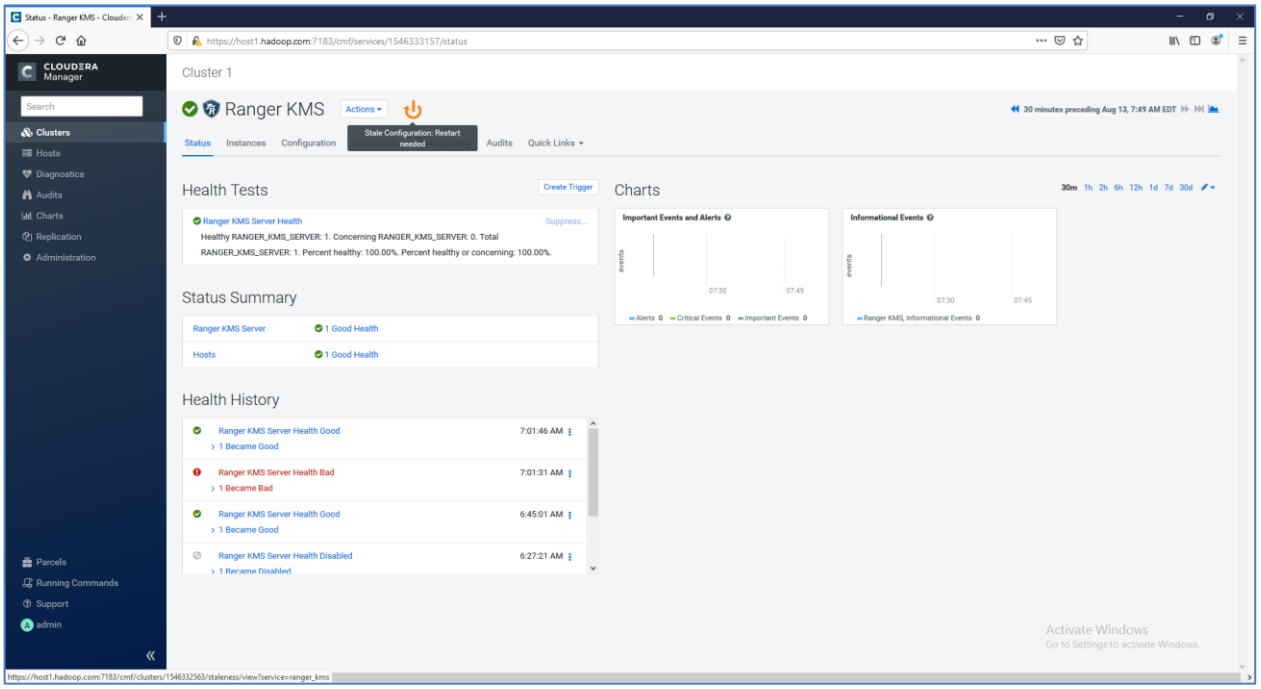
Value: `userpin1`

Description: `Luna HSM Partition Password`

Ensure that the Name/Value pair is entered correctly and change the Partition Name and Partition Password value as per your settings. After entering all the details, click **Save Changes (CTRL+S)**.

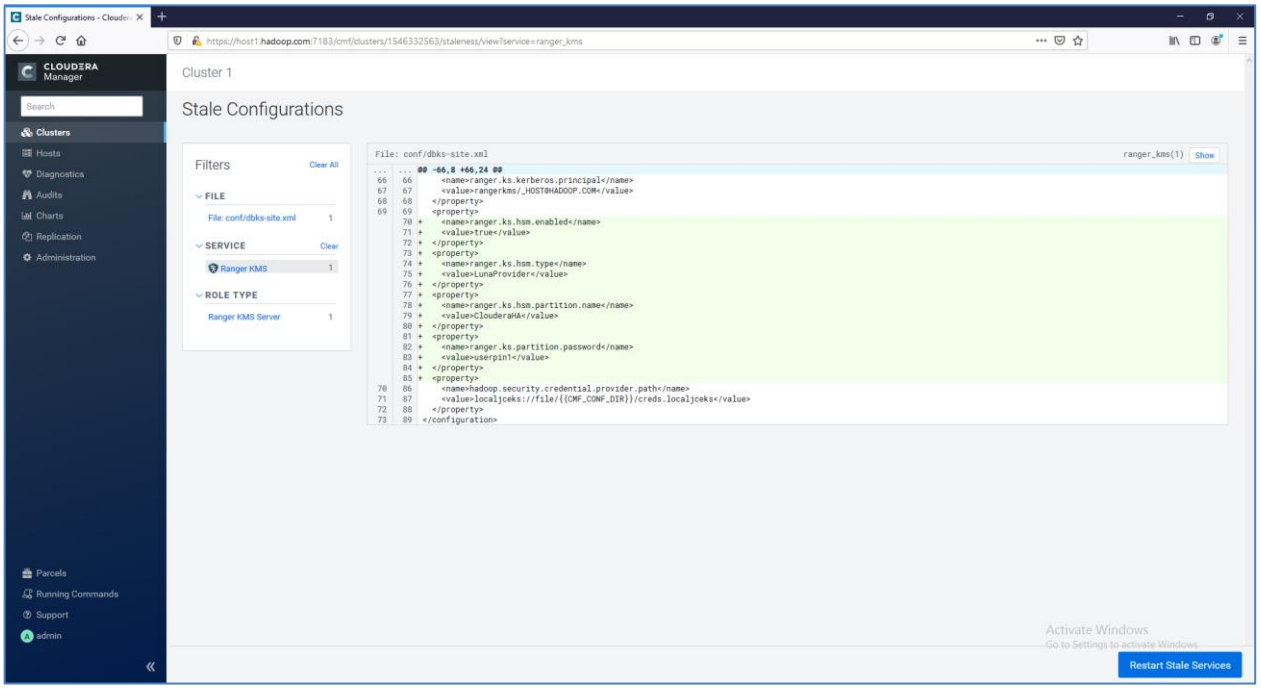


20. After the changes are saved, click on Cloudera Manager icon in the left pane to go back to Cluster Home page. Click **Ranger KMS** service and then click the restart icon to restart the service.

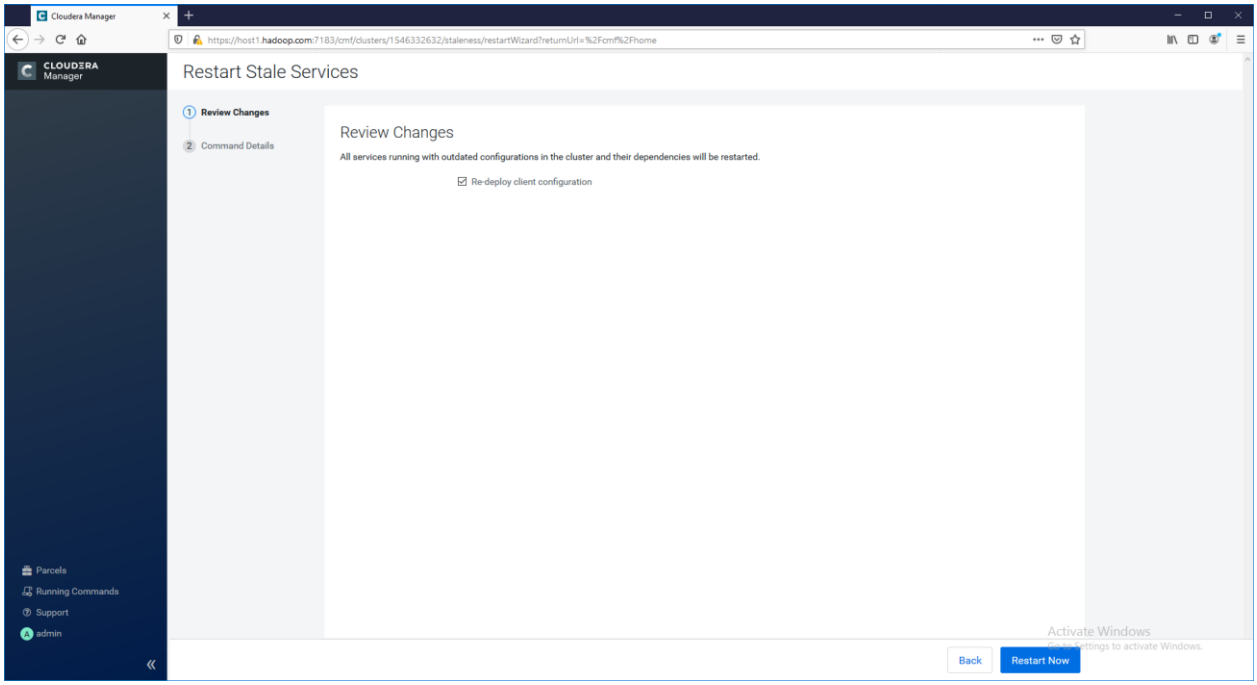


NOTE: Ensure that kms user is added to the hsmusers group.

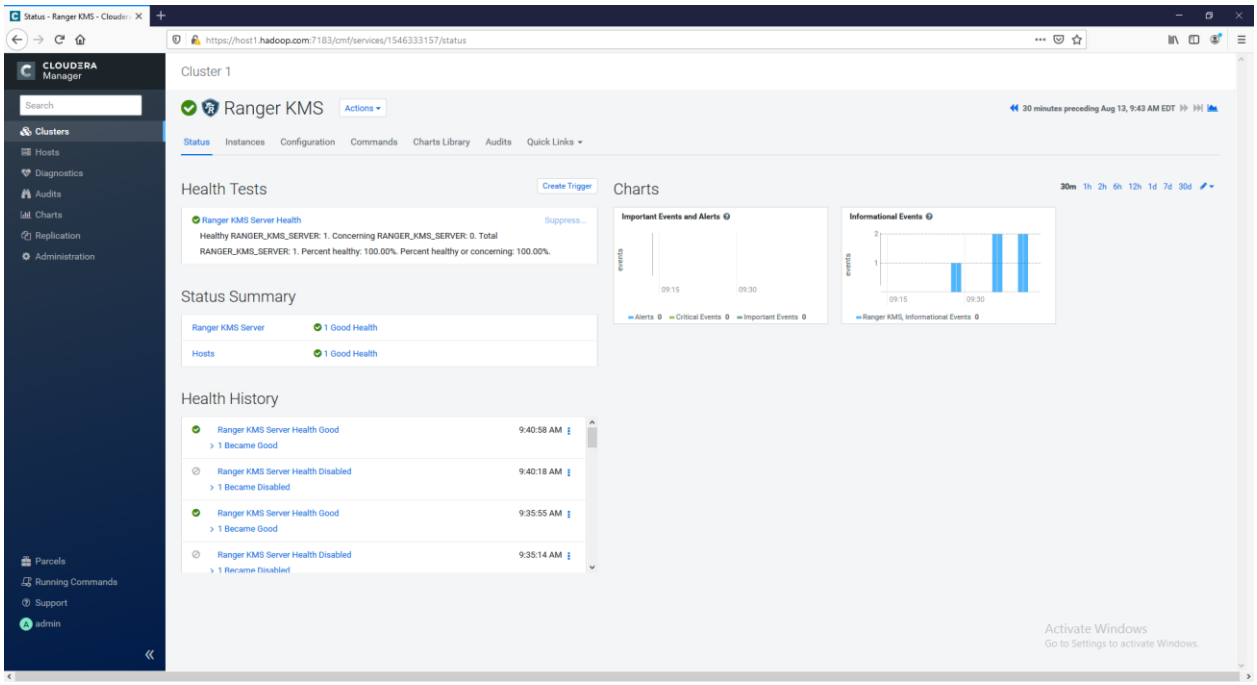
21. On Stale Configuration page, review the changes done in dbks-site.xml and click **Restart Stale Service.**



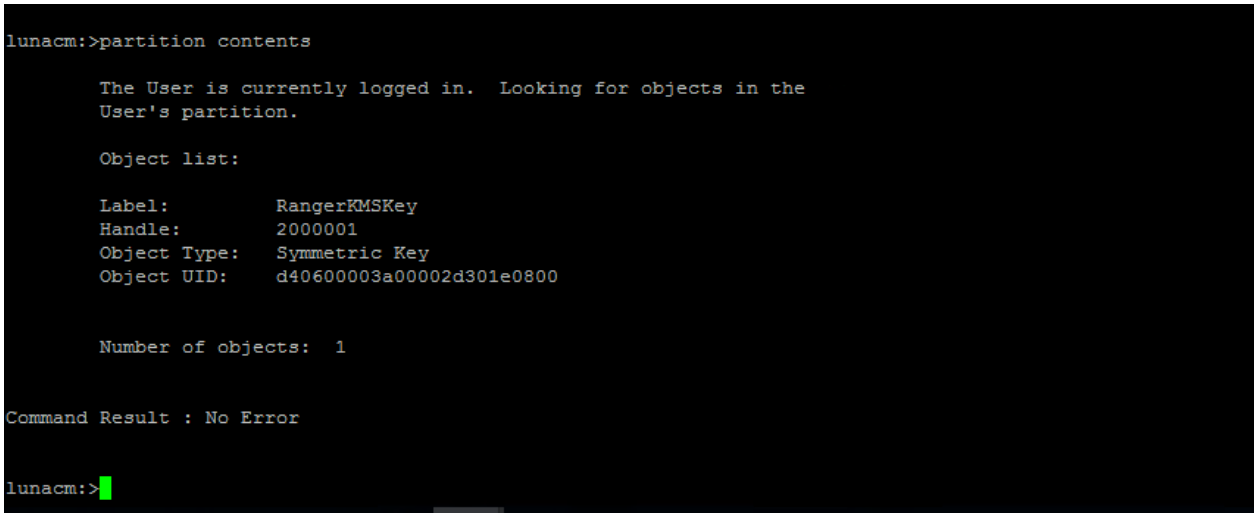
22. On **Review Changes** page, select **Re-deploy client configuration** and click **Restart Now**.



23. Click **Close** when all the services have restarted successfully. You will see the green tick when the Ranger KMS gets started.



24. Run the **lunacm** utility and check the partition contents for generated key.



This completes the integration of Cloudera Data Platform with a Luna HSM. This integration demonstrates configuring the Ranger KMS to use a master key generated and stored on a HSM. Refer the Cloudera Documentation for enabling HDFS Transparent Data Encryption.

Initializing Ranger KMS with Key Trustee Server to use Thales Luna HSM

This section demonstrates the process of initializing the Ranger KMS with Key Trustee Server to use Thales Luna HSM for generating the encryption zone keys stored on Luna Partition. It is assumed that you have installed and configured the Cloudera Manager and setup a cluster with required services up and running in the cluster. Luna Client is installed and configured on the host where you have installed or planning to install the Key Trustee Server.

To configure Ranger KMS with Key Trustee Server to use Thales Luna HSM

1. In a web browser, go to http://<server_host>:7180, where <server_host> is the FQDN or IP address of the host where the Cloudera Manager Server is running.

   NOTE: If you enabled auto-TLS, you are redirected to https://<server_host>:7183, and a security warning is displayed. You may need to indicate that you trust the certificate, or may need to click to proceed to the Cloudera Manager Server host.

2. Log into Cloudera Manager Admin Console. The default credentials are:

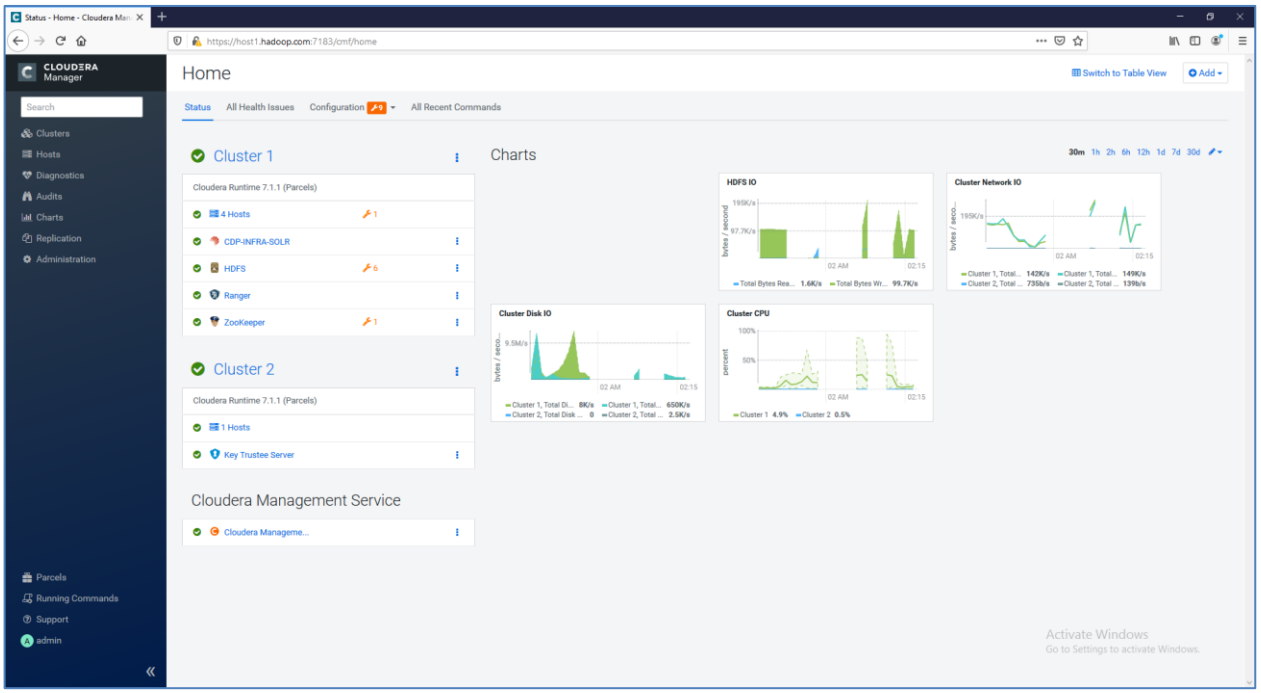
   Username: `admin`

   Password: `admin`

   NOTE: Cloudera Manager does not support changing the admin username for the installed account. You can change the password using Cloudera Manager after you run the installation wizard. Although you cannot change the `admin` username, you can add

a new user, assign administrative privileges to the new user, and then delete the default `admin` account.

3. Ensure that required cluster services are up and running and Key Trustee Server is installed and running in separate cluster as recommended by Cloudera.



NOTE: For demonstration purpose, a stand-alone Key Trustee Server has been set up. Please refer the Cloudera Documentation to set up Key Trustee Server in HA.

4. Log on to the Key Trustee Server host and install the Key HSM. To install the Key HSM, you need to download the Key Trustee Key HSM package from Cloudera and set up local package repository. Refer the Cloudera Documentation to download Key HSM and set up local package repository.

NOTE: If the downloaded package is RPM file then run the command similar to the following to install the downloaded RPM.

```
# yum localinstall keytrustee-keyhsm-7.1.7.7.1.7.0-551.x86_64.rpm
```

```
# yum install keytrustee-keyhsm
--------------------------------------------------------------------------------
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: centos.mirror.snu.edu.in
* epel: fedora.ipserverone.com
* extras: centos.mirror.snu.edu.in
* updates: centos.mirror.snu.edu.in
cloudera-repo1                                                | 2.9 kB
00:00:00
```

```
cloudera-repo1/primary_db                                          | 1.8 kB
00:00:00

Resolving Dependencies

--> Running transaction check

--> Package keytrustee-keyhsm.x86_64 0:7.1.0-
1.keytrustee7.1.0.p0.2758640.el7 will be installed

--> Finished Dependency Resolution


Dependencies Resolved


================================================================================
========================

Package              Arch    Version                          Repository
   Size

================================================================================
========================

 Installing:

 keytrustee-keyhsm     x86_64     7.1.0-1.keytrustee7.1.0.p0.2758640.el7
  cloudera-repo1         16 M


 Transaction Summary

================================================================================
========================


 Install  1 Package


 Total download size: 16 M

 Installed size: 19 M

 Is this ok [y/d/N]: y

 Downloading packages:

 keytrustee-keyhsm-7.1.0-1.keytrustee7.1.0.p0.2758640.el7.x86_64.rpm
  |  16 MB   00:00:00

 Running transaction check

 Running transaction test

 Transaction test succeeded

 Running transaction

 Installing : keytrustee-keyhsm-7.1.0
  1.keytrustee7.1.0.p0.2758640.el7.x86_64                  1/1
```

```
Verifying  : keytrustee-keyhsm-7.1.0-
  1.keytrustee7.1.0.p0.2758640.el7.x86_64                    1/1


Installed:
keytrustee-keyhsm.x86_64 0:7.1.0-1.keytrustee7.1.0.p0.2758640.el7


Complete!
[root@host5 cm7]#
```

Cloudera Navigator Key HSM is installed to the /usr/share/keytrustee-server-keyhsm directory by default.

5. Ensure that the HSM client libraries are installed on the Key HSM host and HSM is properly configured and accessible from the Key HSM host.

```
# /usr/safenet/lunaclient/bin/vtl listslots
-------------------------------------------------------------------------------
vtl (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.

Number of slots: 1

The following slots were found:

Slot Description          Label          Serial #         Status
==== ==================== ============== ================ ============
   0 HA Virtual Card Slot ClouderaHA     11238696044945   Present
-------------------------------------------------------------------------------
```

> **NOTE:** Ensure that keyhsm user is added to hsmusers group. If you are running Key Trustee Server in HA, Key HSM must be setup with Luna HSM for all host running Key Trustee Server.

6. Initialize the Key HSM in conjunction with Luna HSM using the command below.

```
# service keyhsm setup luna
-------------------------------------------------------------------------------
Configuring keyHsm General Setup
Cloudera recommends to use 127.0.0.1 as the listener port for Key HSM
Please enter Key HSM SSL listener IP address: [127.0.0.1]127.0.0.1
Will attempt to setup listener on 127.0.0.1
Please enter Key HSM SSL listener PORT number: 9090


validate Port:                                    :[ Successful ]
```

```
-- Configuring SafeNet Luna HSM --

Please enter SafeNetHSM Slot Number: 0

Please enter SafeNet HSM password (input suppressed):

Configuration stored in: 'application.properties'. (Note: You can also use
keyhsm settings to quickly view your current configuration)


Configuration saved in 'application.properties' file

------------------------------------------------------------------------
```

7. After the setup is completed, the Key HSM configuration is stored in **/usr/share/keytrustee-server-keyhsm/application.properties**. You can validate the settings using the `service keyhsm settings` command.

```
# service keyhsm settings

------------------------------------------------------------------------

# keyHsm Server Configuration information:

keyhsm.management.address : 127.0.0.1

keyhsm.server.port : 9090

keyhsm.management.port : 9899

keyhsm.service.port : 19791

keyhsm.hardware : luna


# Luna HSM Configuration

hsm.luna.login :
TJ/xlxO1nbJittzRWHD/a7bZ+ppBv/w+aMq9OzKtUUneSSSU6R+Qtd/Y2J9q8iCzXUVfxKaPH+3
Gs+ZrUOVfkDVyvYG+y/bM8hVqDcwmf1nnpv/aUknKfEgnpp44vZZNQD9Tf+zOlchr90Kbb4qr17
jWHYje+vfxsPT8cQ5w36iqRJBZq7nIQ4dY/qireBMzdrO1mCS8e9qsg8u5qmejkOv00oesHRoXS
bNbBHnaDb044SxtKRyhNrKVPYU5Hk4c18Q/4zfvIZiXGIWM6SdKGq/Ul44E6BQoS/5/t5PhIn5Y
J3yoi5RK4U3ah2pJJOiz/mQBxHK8Llxnv74DO+xYhg==

hsm.luna.slot : 0

------------------------------------------------------------------------
```

8. Key HSM service must explicitly trust the Key Trustee Server certificate (presented during TLS handshake). To establish this trust, run the following command:

```
# keyhsm trust /var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee.pem
```

> **NOTE:** If Key Trustee Server uses a custom certificate (obtained from a commercial or internal CA) instead of default certificate, provide the path to the custom certificate.

9. Start the Key HSM service.

```
# service keyhsm start

------------------------------------------------------------------------

Starting KeyHSM, please wait...
```

```
KeyHSM started successfully

-------------------------------------------------------------------
```

10. Establish trust from Key Trustee Server to Key HSM specifying the path to the private key and certificate (Key Trustee Server is a client to Key HSM). This example shows how to use the **--client-certfile** and **--client-keyfile** options to specify the path to default certificate and key.

```
# ktadmin keyhsm --server https://127.0.0.1:9090 --client-certfile
/var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee.pem --client-
keyfile /var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee-pk.pem --
trust
```

> **NOTE:** For a password-protected Key Trustee Server private key, add the --passphrase argument to the command and enter the password when prompted.

For Example:

```
# ktadmin keyhsm --passphrase --server https://127.0.0.1:9090 --client-
certfile  /var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee.pem --
client-keyfile /var/lib/keytrustee/.keytrustee/.ssl/ssl-cert-keytrustee-
pk.pem --trust

-------------------------------------------------------------------------

INFO:root:Skipping cert creation (file exists)

Enter the Passphrase of the Private Key of the SSL Certificate:


KeyHSM Setup Completed Successfully!


Key Trustee Server configured to use KeyHSM server @ https://127.0.0.1:9090

Please restart Key Trustee Server for these changes to take effect.

-------------------------------------------------------------------------
```

Any keys that exist on the Key Trustee Server are automatically migrated when you run the **ktadmin keyhsm** command. To complete the migration, enter **y** or **yes** at the command prompt:

```
-------------------------------------------------------------------------

Some deposits were found that will need to be moved to the HSM.

        Note that although this operation can be interrupted, once
complete,

        items stored in the HSM must remain there!


Do you want to perform this migration now? [y/N]: y

Migrating hsm deposits...

Migration Complete!

-------------------------------------------------------------------------
```

11. Log in to the Cloudera Management Console and restart Key Trustee Server (**Key Trustee Server** service > **Actions** > **Restart**).

12. Verify connectivity between the Key HSM service and the Luna HSM using the following command.

```
# curl -k https://host5.hadoop.com:11371/test_hsm
```

Successful connection and test of operations returns output like the following:

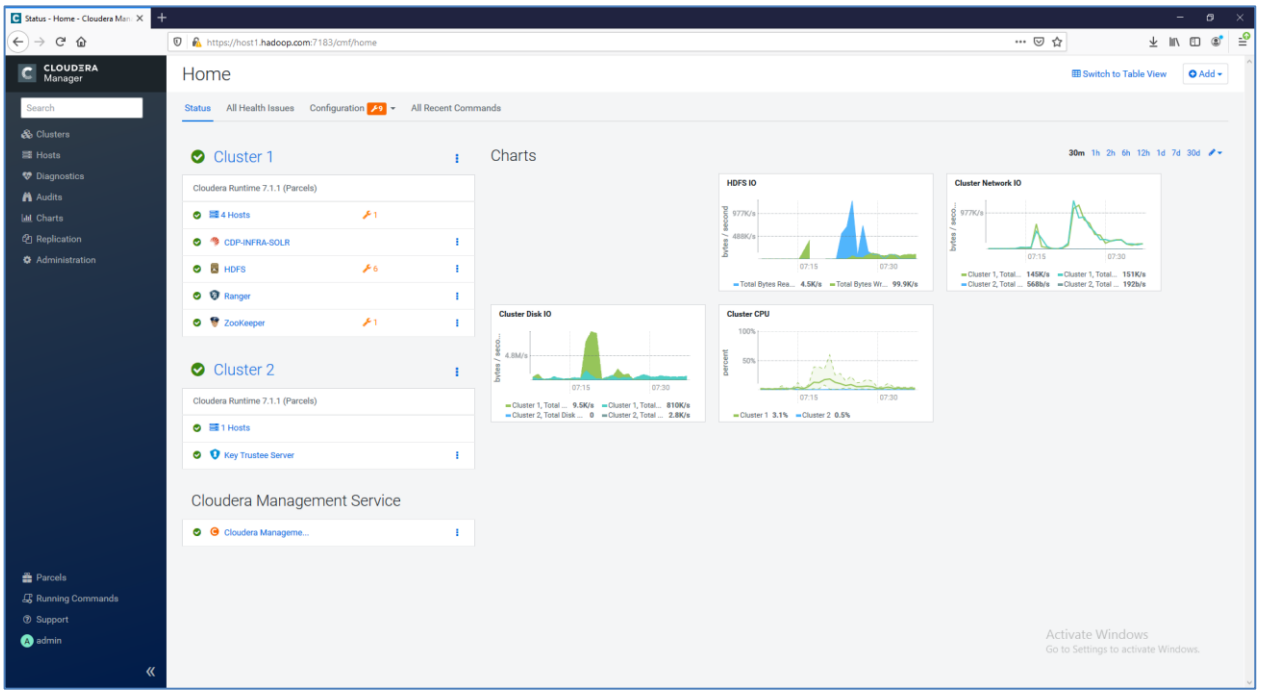
```
-------------------------------------------------------------------------------------------------------------------------------

"Sample Key TEST_HELLO_DEPOSIT2020-09-01-134034 has been created"

-------------------------------------------------------------------------------------------------------------------------------
```

> **NOTE:** If you are using the test_hsm script to verify that the Key Hardware Security Module (Key HSM) has successfully integrated with the Key Trustee Server, or to verify that the Key HSM is connected to HSM, and the Key Trustee Server private key file is password-protected, then the verification may fail. This can occur even if the integration is successful or connected.
>
> If this occurs, you need to create a key through Hadoop for the test.

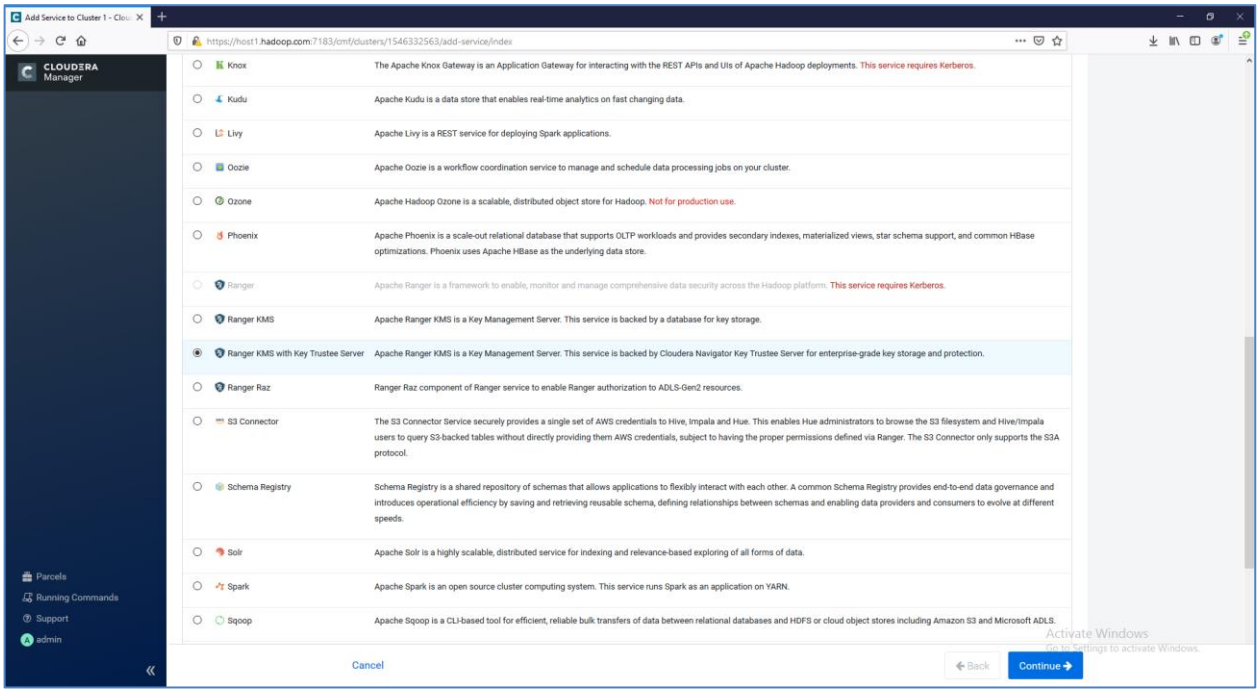
13. Before you begin the installation on **Ranger KMS with Key Trustee Server**, ensure that:

- Apache Ranger is installed and running.
- Key Trustee Server is installed and running.

On the cluster **Home** page, click the **More Options** icon (•••), and then click **Add Service**.

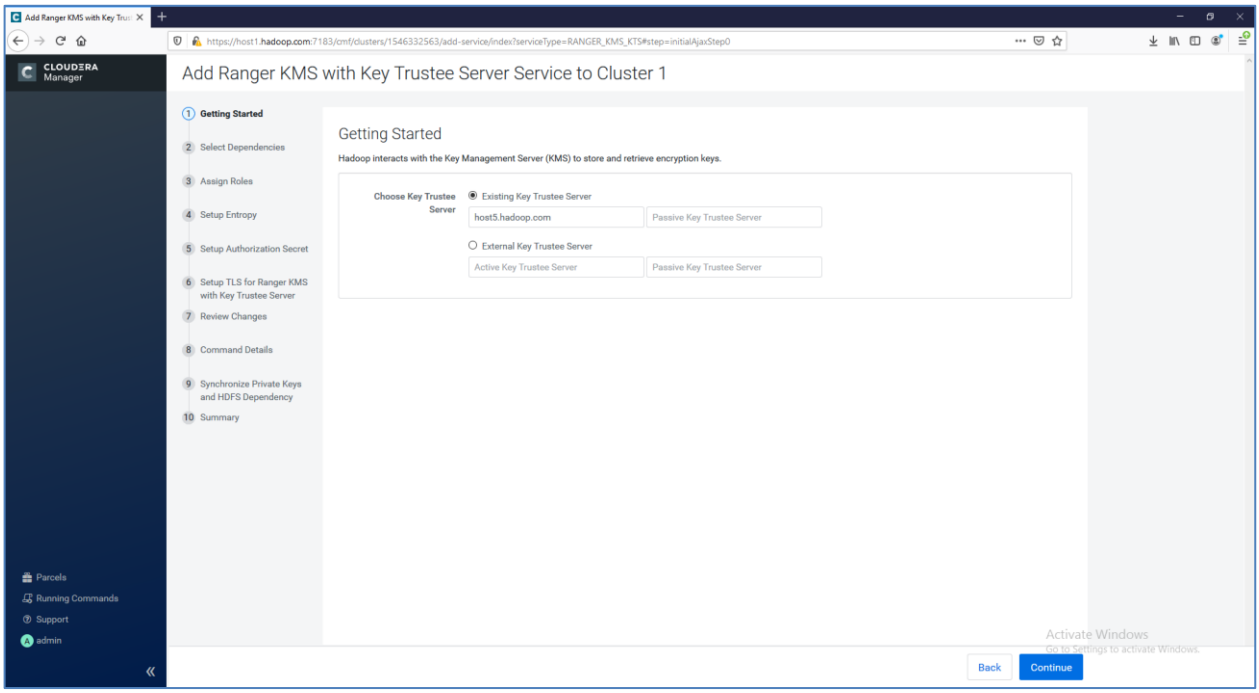


14. Select **Ranger KMS with Key Trustee Server** and click **Continue**.



15. A wizard will open to Add Ranger KMS with Key Trustee Server Service to the cluster. Use the wizard to install Ranger KMS with Key Trustee Server.

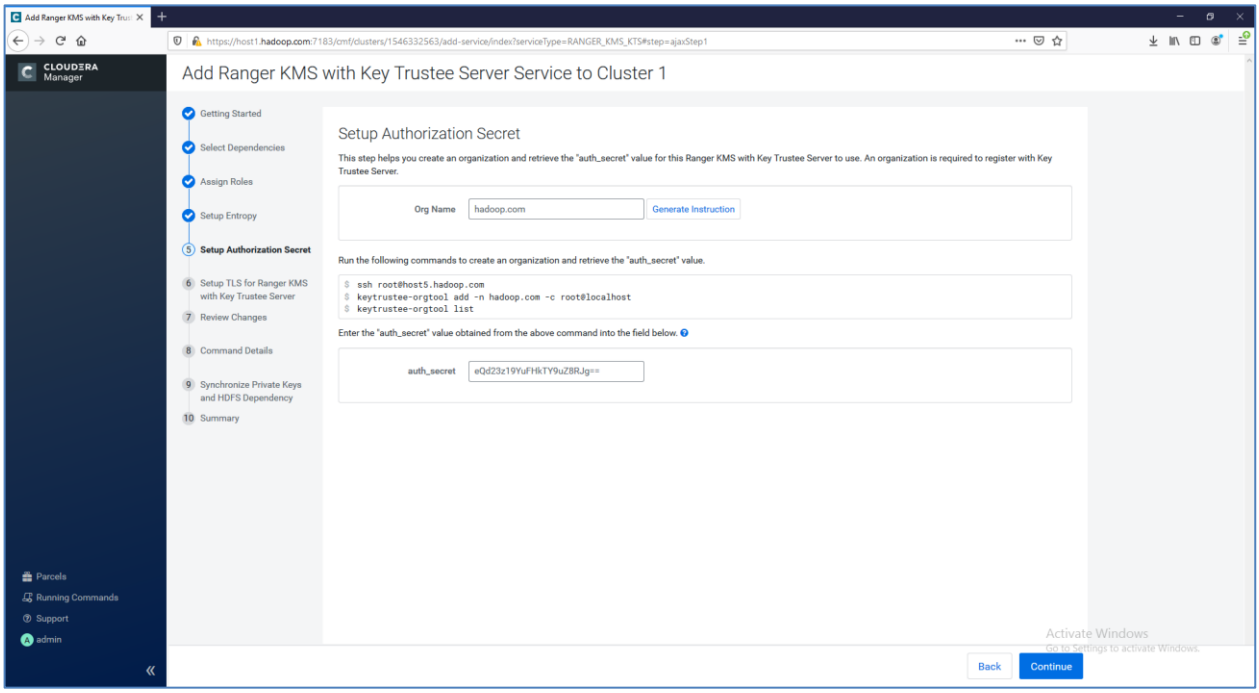
16. On **Getting Started** page, Select the Existing Key Trustee Server and click **Continue**.



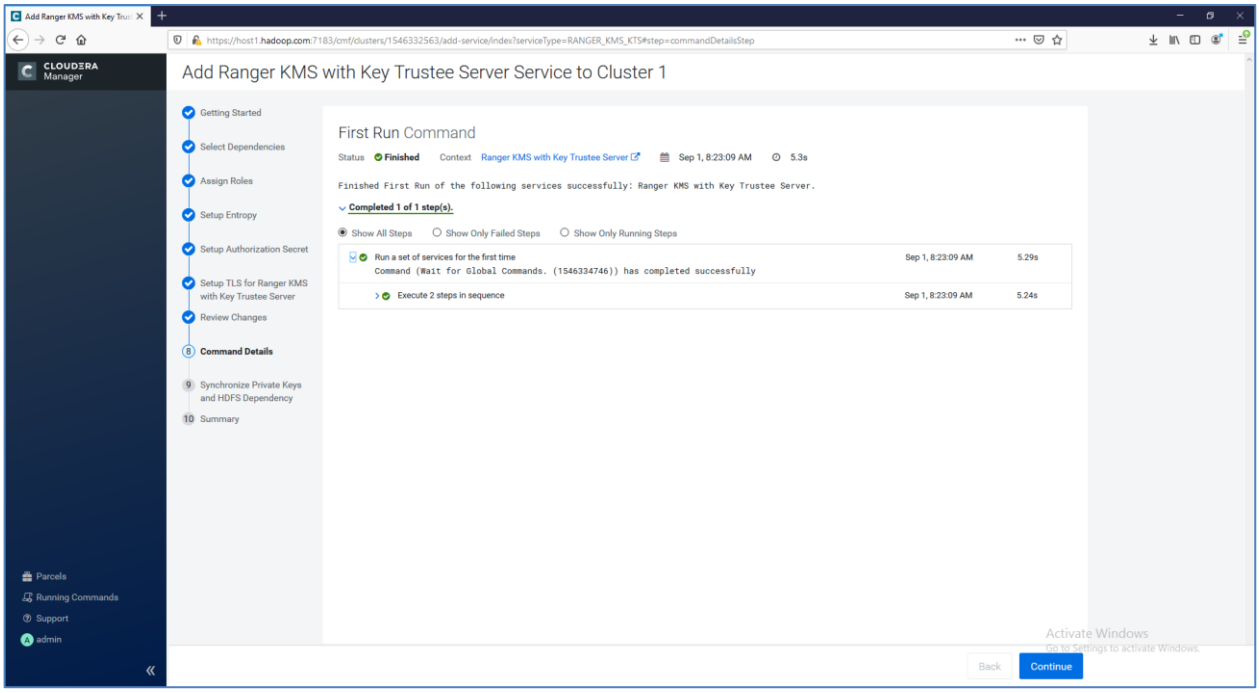
17. On **Assign Roles** page, select the host on which the service will be installed and click **Continue**.

18. On **Setup Entropy** page, check the entropy on selected host and if required follow the instructions provided on the page to set up required entropy. Click **Continue**.

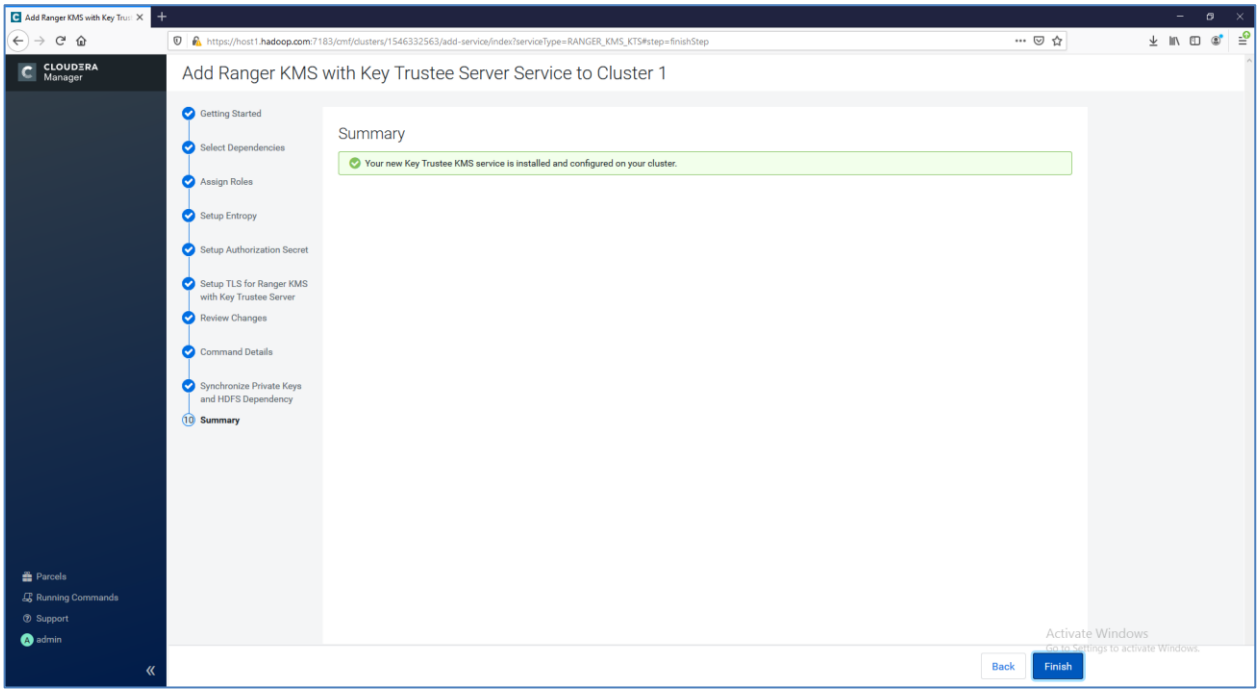
19. On **Setup Authorization Secret** page, enter the **Org Name** and click **Generate Instructions**. Follow the instructions to retrieve the "auth_secret" value. Enter the **auth_secret** and click **Continue**.



20. On **Setup TLS for Ranger KMS with Key Trustee Server** page, click **Continue** to proceed.
21. On **Review Changes** page, click **Continue** to proceed.
22. Wait for the command to finish and set up the service and then click **Continue** to proceed.

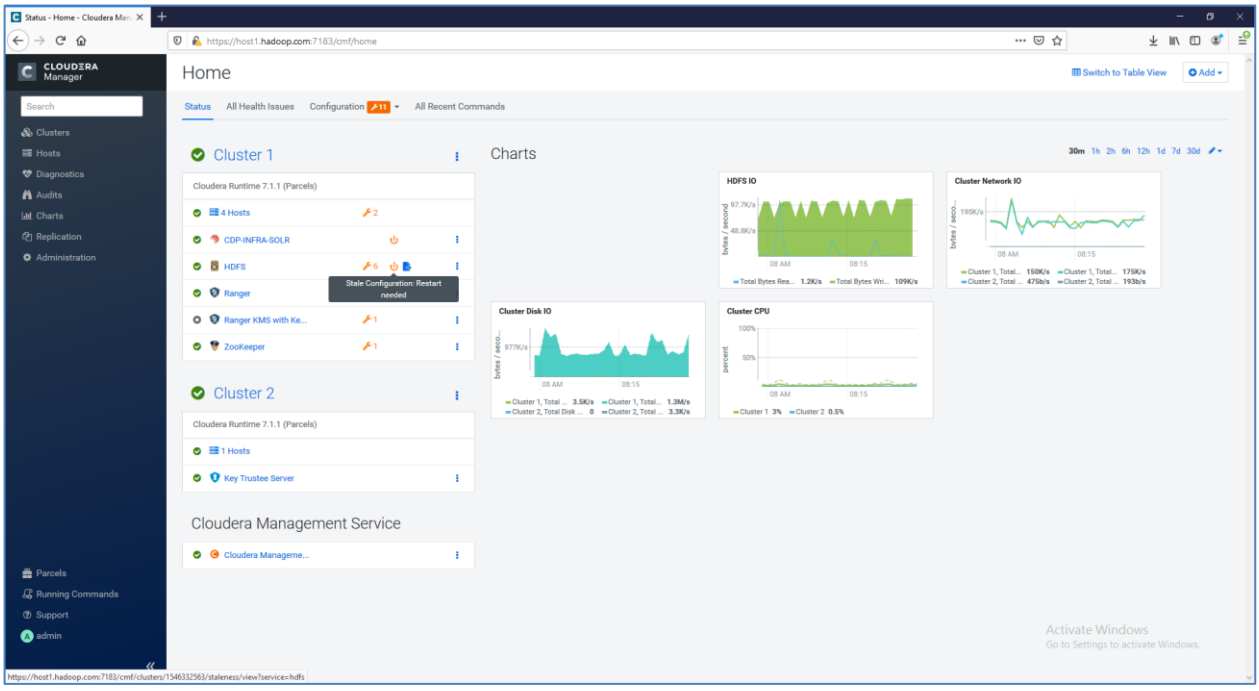


23. Click **Continue** and then click **Finish**.

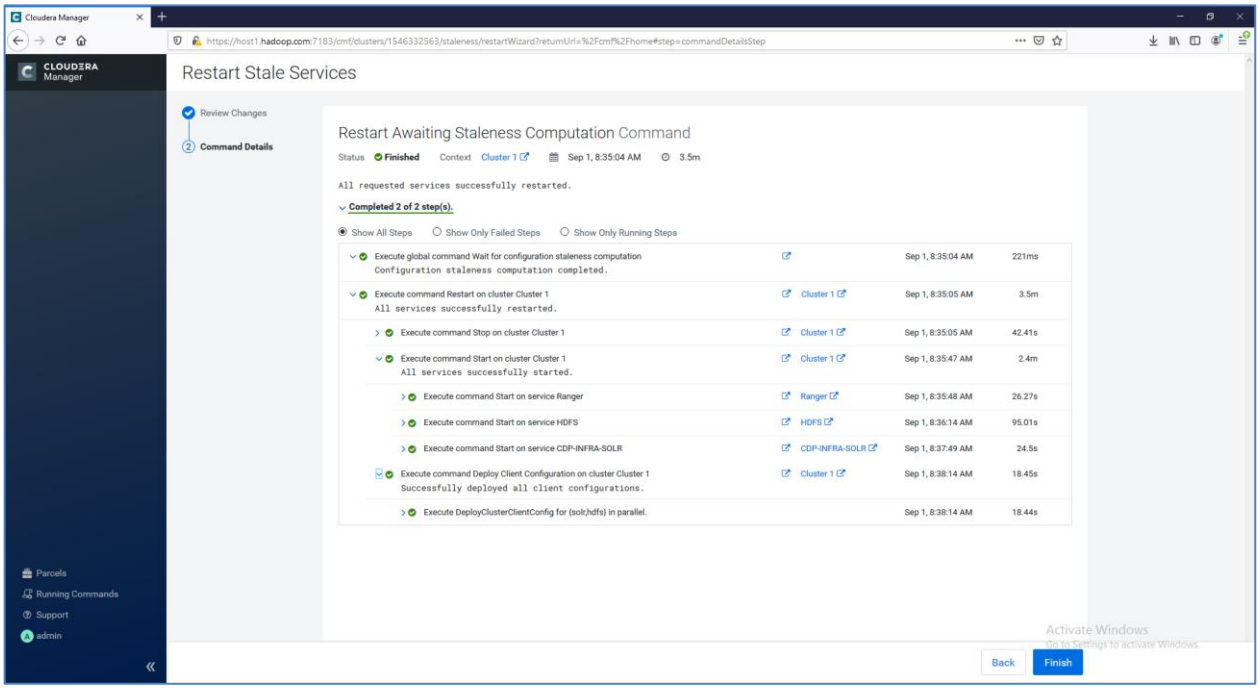


NOTE: If more than one KMS instance is configured. See Cloudera Documentation for "Upgrading Key Trustee KMS" for guidance on synchronization and validation of private keys. If keys are not synchronize on all instances then Ranger KSM with Key Trustee Server will not start.

24. Click on Stale Configuration to restart the services and then **Restart Stale Services**.

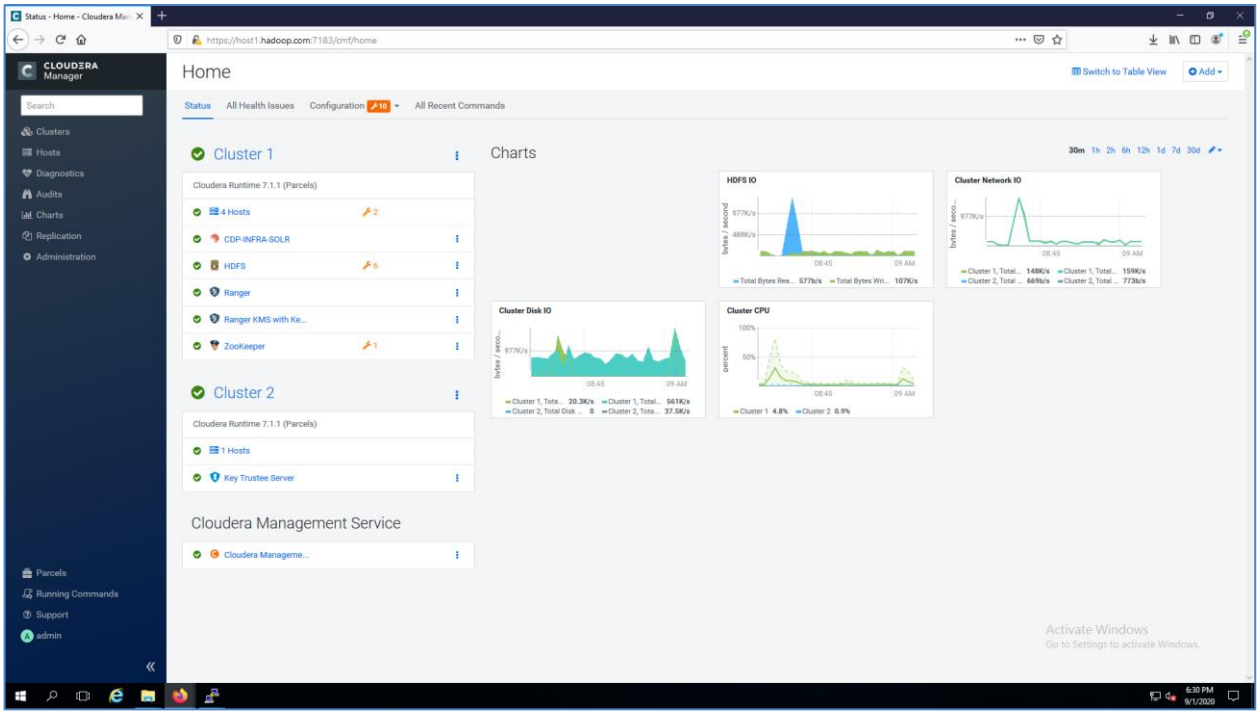


25. On the **Restart Stale Services** page. Click **Restart Now**. When the Services restart successfully, click **Finish**.

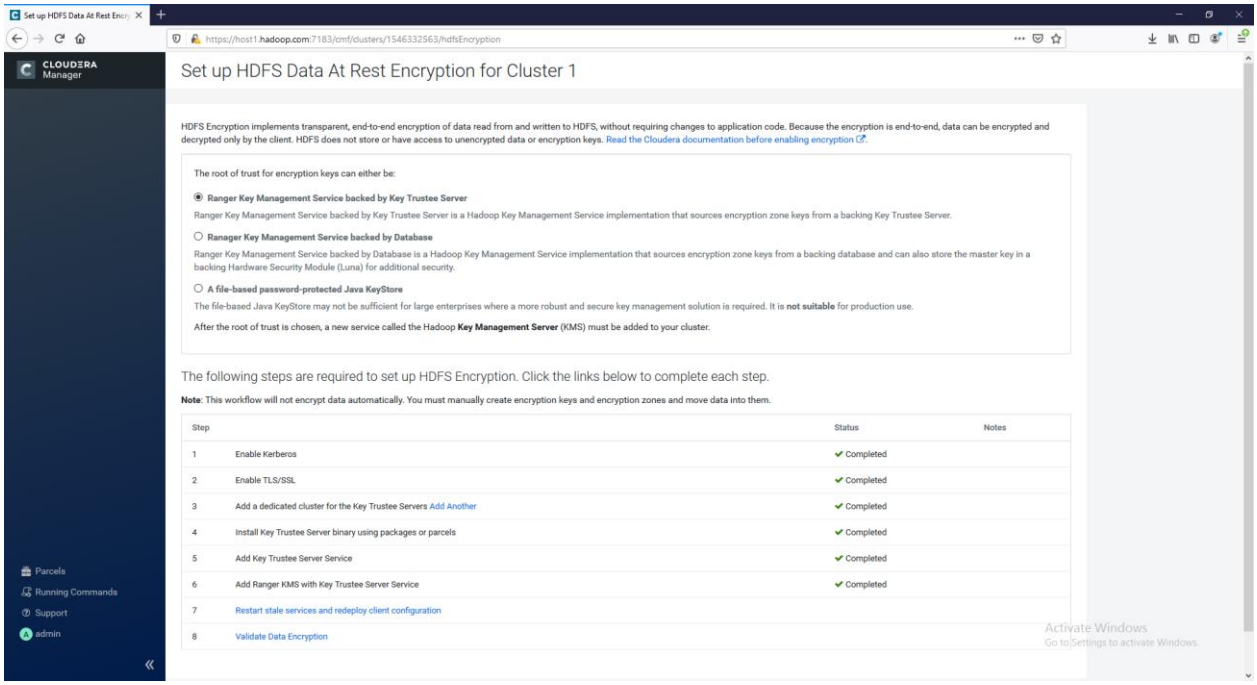


26. Start Ranger KMS with Key Trustee Server (**Ranger KMS with Key Trustee Server** service > **Actions** > **Start**).

27. Ensure that service starts successfully and is running on Cluster Home page.



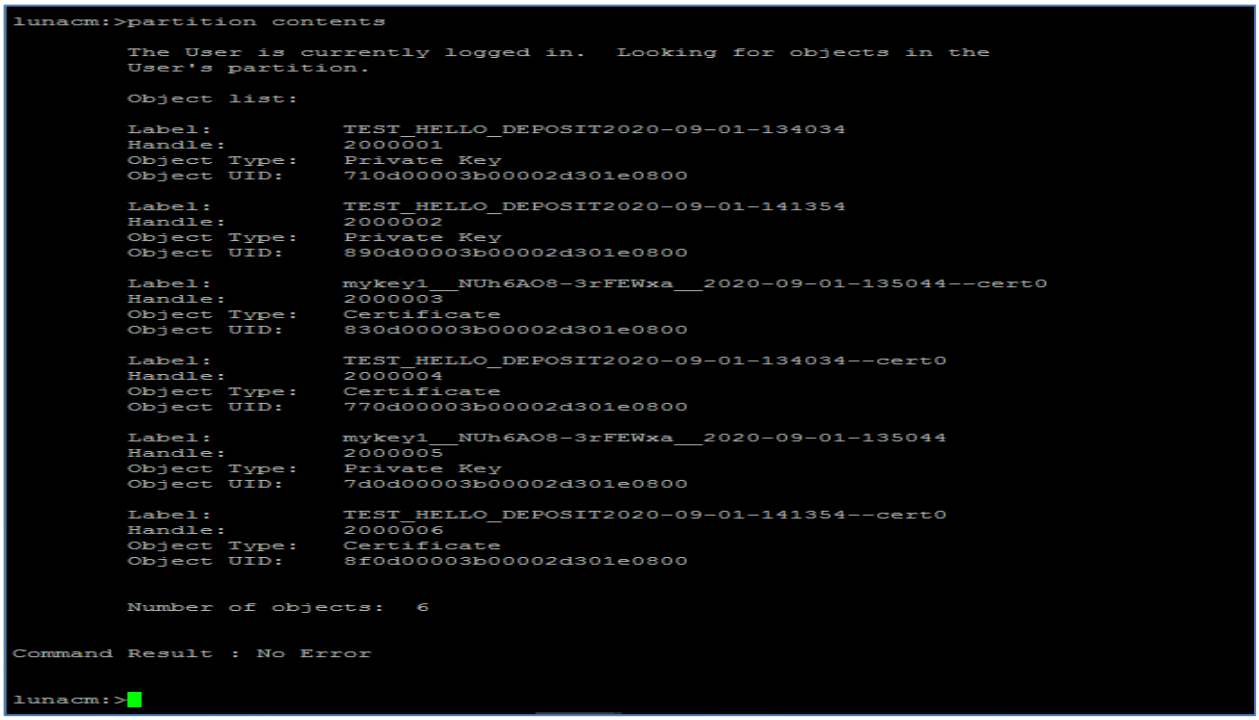
28. On the cluster **Home** page, click the More Options icon (⋯) and then click **Set up HDFS Data At Rest Encryption**. Select **Ranger Key Management Service backed by Key Trustee Server** and click **Validate Data Encryption**. Run the instructions provided in **Validate Data Encryption** window.



29. Refer the Cloudera Documentation for enabling HDFS Transparent Data Encryption. When the instructions are executed, the Encryption Key gets created on Luna HSM and is used to encrypt/decrypt the file in the encrypted key zone.

```
[root@host1 ~]# kinit kms
Password for kms@HADOOP.COM:
[root@host1 ~]# hadoop key create mykey1
mykey1 has been successfully created with options Options{cipher='AES/CTR/NoPadding', bitLength=128, description='null', attributes=null}.
org.apache.hadoop.crypto.key.kms.LoadBalancingKMSClientProvider@5fb759d6 has been updated.
[root@host1 ~]# hadoop fs -mkdir /tmp/zone1
[root@host1 ~]# kinit hdfs
Password for hdfs@HADOOP.COM:
[root@host1 ~]# hdfs crypto -createZone -keyName mykey1 -path /tmp/zone1
Added encryption zone /tmp/zone1
[root@host1 ~]# kinit kms
Password for kms@HADOOP.COM:
[root@host1 ~]# echo "Hello World" > /tmp/helloWorld.txt
[root@host1 ~]# hadoop fs -put /tmp/helloWorld.txt /tmp/zone1
[root@host1 ~]# hadoop fs -cat /tmp/zone1/helloWorld.txt
Hello World
[root@host1 ~]# rm /tmp/helloWorld.txt
rm: remove regular file '/tmp/helloWorld.txt'? y
[root@host1 ~]# kinit hdfs
Password for hdfs@HADOOP.COM:
kinit: Password incorrect while getting initial credentials
[root@host1 ~]# kinit hdfs
Password for hdfs@HADOOP.COM:
[root@host1 ~]# hadoop fs -cat /.reserved/raw/tmp/zone1/helloWorld.txt
[root@host1 ~]# hadoop fs -rm -R /tmp/zone1
20/09/01 14:07:20 INFO fs.TrashPolicyDefault: Moved: 'hdfs://host2.hadoop.com:8020/tmp/zone1' to trash at: hdfs://host2.hadoop.com:8020/user/hdfs/.Trash/Current/tmp/zone1
[root@host1 ~]#
```

30. Run the **lunacm** utility and check the partition contents. You will see the keys get generated every time when HSM connectivity with Luna HSM is being checked using curl command or when we run Hadoop command to create the keys.



This completes the integration of Cloudera Data Platform with a Luna HSM. This integration demonstrates how to configure the Ranger KMS with Key Trustee Server that uses the Key HSM to create encryption zone keys on Luna HSM.

Contacting Customer Support

If you encounter a problem at any stage during this integration, contact Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.