Cloudera Data Platform

INTEGRATION GUIDE

THALES LUNA HSM

Document Information

Document Part Number	007-000730-001
Revision	A
Release Date	4 December 2020

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 Cloudera Manager Version

The integration of Cloudera Data Platform with Luna HSM is certified on Cloudera Manager v7.1.1.

> **NOTE:** You can use any Luna Client version along with the supported Luna HSM can be used, provided Cloudera Runtime, Ranger KMS, Key Trustee Server, and Luna HSM are supported.

Prerequisites

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

Configure Thales Luna HSM

Set up and configure Thales Luna HSM device for your system. Refer to the *Thales Luna HSM Product Documentation* for help.

1. Ensure the HSM is setup, initialized, provisioned, and ready for deployment.
2. Create a partition on the HSM for use by Cloudera Service.
3. If using a Thales Luna Network HSM, register a client for the system and assign the client to a partition to create an NTLS connection.
4. Initialize the Crypto Officer and Crypto User roles for the initialized partition.
5. Verify that the partition is successfully registered and configured. The command to see the registered partition 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
```

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

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 Thales Luna HSM High-Availability (HA)

Refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stops functioning for some reason, all the calls are automatically routed to secondary till primary starts functioning again.

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.

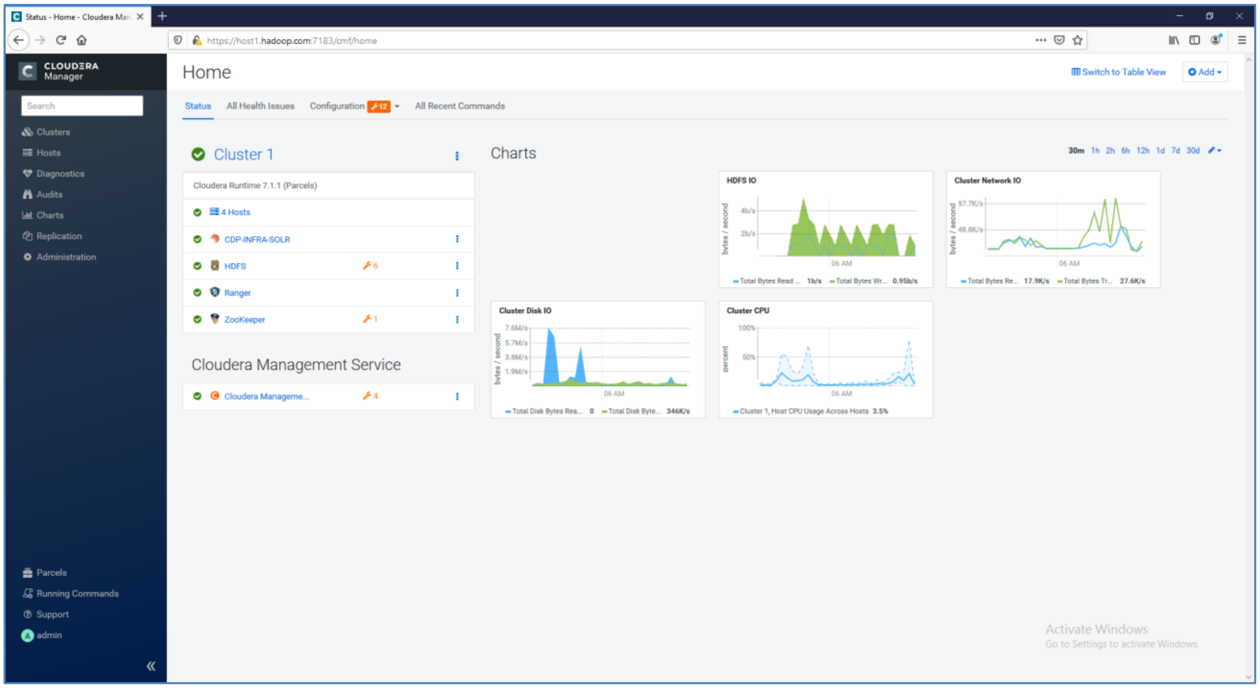
5. Log in to Cloudera Manager Admin console. The default credentials are:

   Username: `admin`

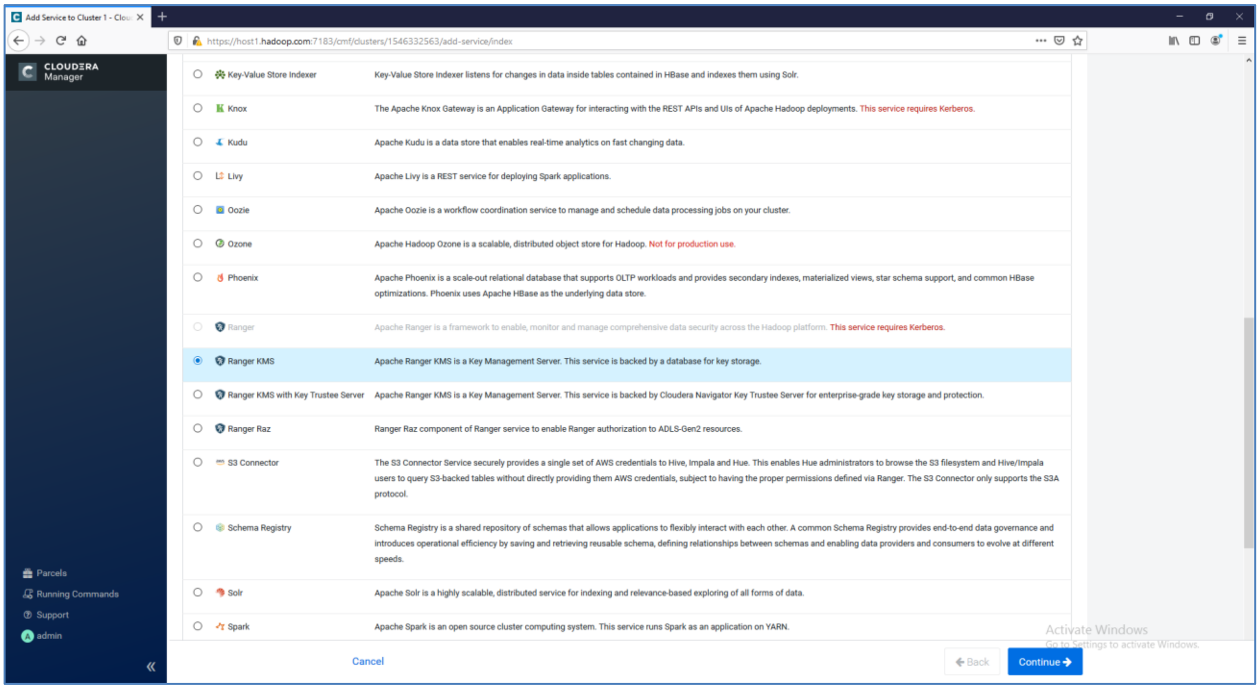
   Password: `admin`

> **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**.


Status - Home - Cloudera Man
https://host1.hadoop.com:7183/cmf/home
CLOUDERA Manager
Search
Clusters
Hosts
Diagnostics
Audits
Charts
Replication
Administration
Parcels
Running Commands
Support
admin
Home
Switch to Table View
Add
Status
All Health Issues
Configuration 12
All Recent Commands
Cluster 1
Cloudera Runtime 7.1.1 (Parcels)
4 Hosts
CDP-INFRA-SOLR
HDFS
6
Ranger
ZooKeeper
1
Cloudera Management Service
Cloudera Manageme...
4
Charts
30m 1h 2h 6h 12h 1d 7d 30d
HDFS IO
Cluster Network IO
Cluster Disk IO
Cluster CPU
bytes / second
percent
06 AM
Total Bytes Read ... 1b/s
Total Bytes Wr... 0.95b/s
Total Bytes Re... 17.9K/s
Total Bytes Tr... 27.6K/s
Total Disk Bytes Rea... 0
Total Disk Byte... 346K/s
Cluster 1, Host CPU Usage Across Hosts 3.5%
Activate Windows
Go to Settings to activate Windows.

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



https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index

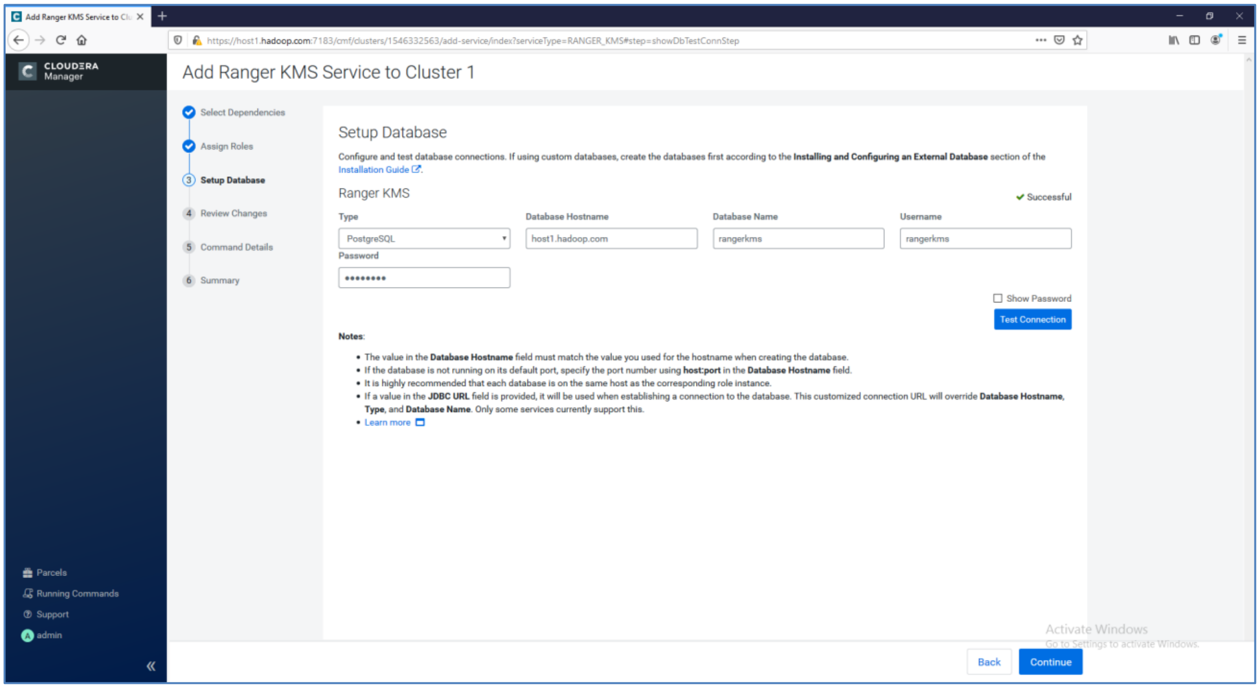
○	Key-Value Store Indexer	Key-Value Store Indexer listens for changes in data inside tables contained in HBase and indexes them using Solr.
○	Knox	The Apache Knox Gateway is an Application Gateway for interacting with the REST APIs and UIs of Apache Hadoop deployments. This service requires Kerberos.
○	Kudu	Apache Kudu is a data store that enables real-time analytics on fast changing data.
○	Livy	Apache Livy is a REST service for deploying Spark applications.
○	Oozie	Apache Oozie is a workflow coordination service to manage and schedule data processing jobs on your cluster.
○	Ozone	Apache Hadoop Ozone is a scalable, distributed object store for Hadoop. Not for production use.
○	Phoenix	Apache Phoenix is a scale-out relational database that supports OLTP workloads and provides secondary indexes, materialized views, star schema support, and common HBase optimizations. Phoenix uses Apache HBase as the underlying data store.
○	Ranger	Apache Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform. This service requires Kerberos.
●	Ranger KMS	Apache Ranger KMS is a Key Management Server. This service is backed by a database for key storage.
○	Ranger KMS with Key Trustee Server	Apache Ranger KMS is a Key Management Server. This service is backed by Cloudera Navigator Key Trustee Server for enterprise-grade key storage and protection.
○	Ranger Raz	Ranger Raz component of Ranger service to enable Ranger authorization to ADLS-Gen2 resources.
○	S3 Connector	The S3 Connector Service securely provides a single set of AWS credentials to Hive, Impala and Hue. This enables Hue administrators to browse the S3 filesystem and Hive/Impala users to query S3-backed tables without directly providing them AWS credentials, subject to having the proper permissions defined via Ranger. The S3 Connector only supports the S3A protocol.
○	Schema Registry	Schema Registry is a shared repository of schemas that allows applications to flexibly interact with each other. A common Schema Registry provides end-to-end data governance and introduces operational efficiency by saving and retrieving reusable schema, defining relationships between schemas and enabling data providers and consumers to evolve at different speeds.
○	Solr	Apache Solr is a highly scalable, distributed service for indexing and relevance-based exploring of all forms of data.
○	Spark	Apache Spark is an open source cluster computing system. This service runs Spark as an application on YARN.

Cancel ← Back 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.



Add Ranger KMS Service to Cluster 1

Setup Database

Configure and test database connections. If using custom databases, create the databases first according to the **Installing and Configuring an External Database** section of the Installation Guide.

Ranger KMS

✓ Successful

Type	Database Hostname	Database Name	Username
PostgreSQL	host1.hadoop.com	rangerkms	rangerkms

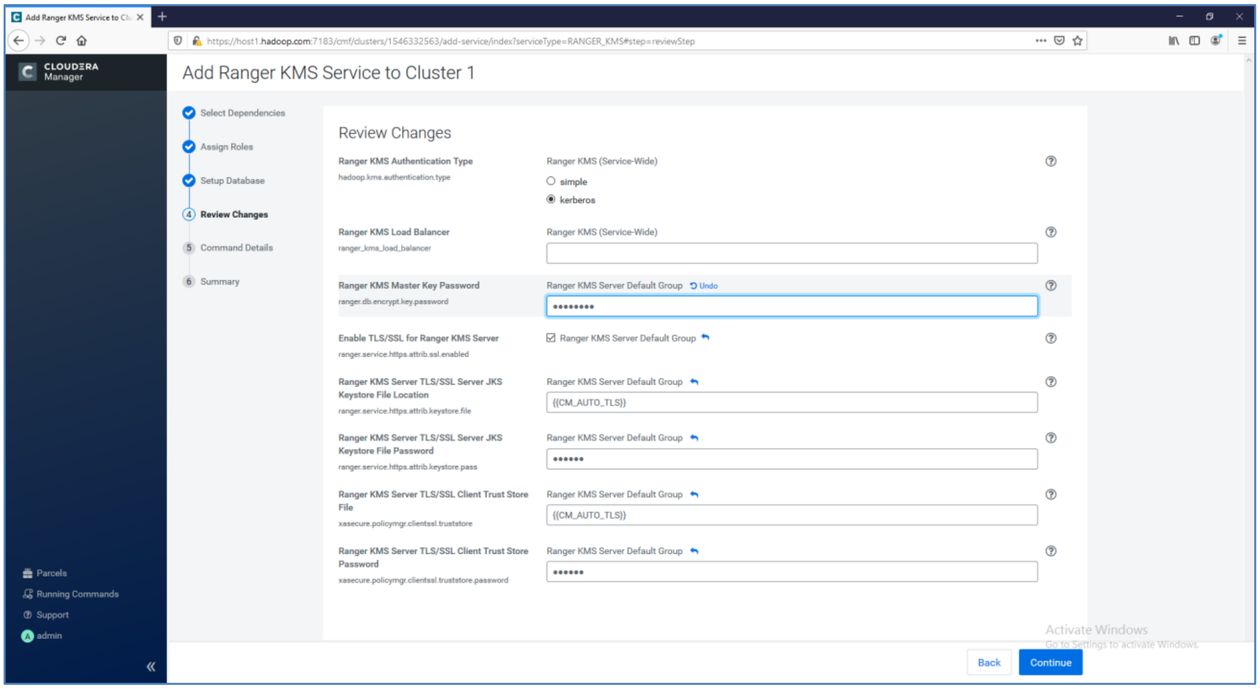
Password: ••••••••

□ Show Password

Notes:

- The value in the **Database Hostname** field must match the value you used for the hostname when creating the database.
- If the database is not running on its default port, specify the port number using **host:port** in the **Database Hostname** field.
- It is highly recommended that each database is on the same host as the corresponding role instance.
- If a value in the **JDBC URL** field is provided, it will be used when establishing a connection to the database. This customized connection URL will override **Database Hostname**, **Type**, and **Database Name**. Only some services currently support this.
- Learn more

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

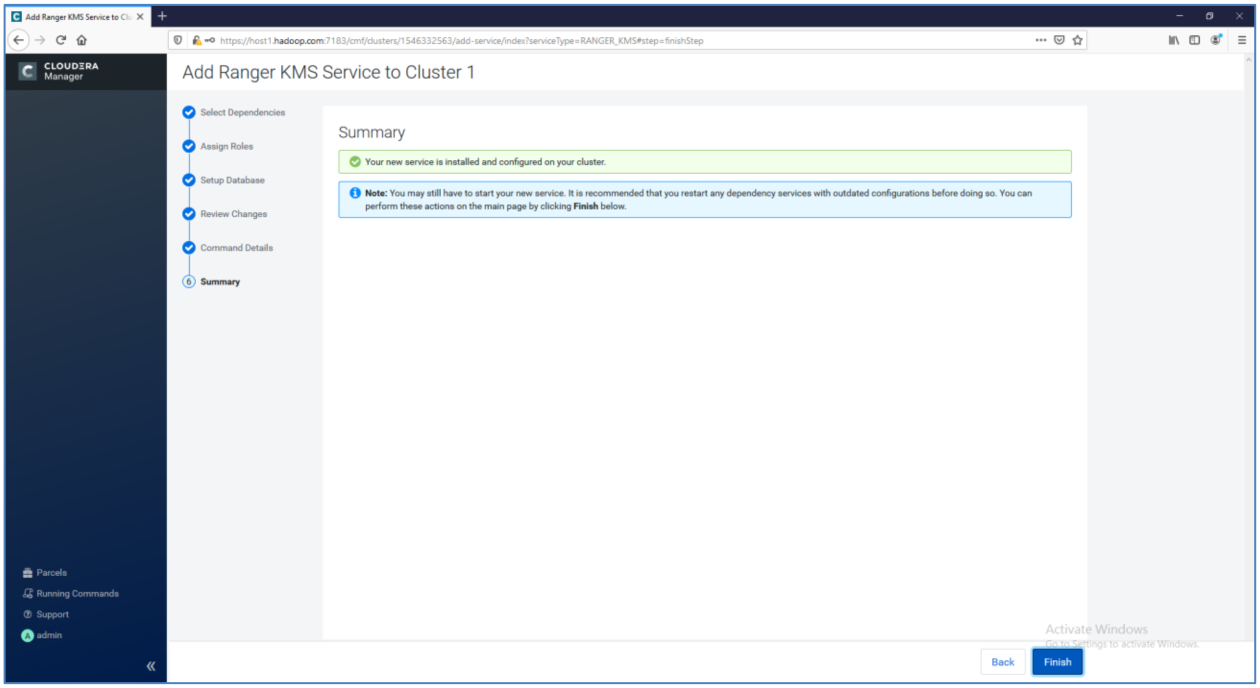

Add Ranger KMS Service to Clu
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index?serviceType=RANGER_KMS#step=reviewStep
CLOUDERA Manager
Select Dependencies
Assign Roles
Setup Database
4 Review Changes
5 Command Details
6 Summary
Parcels
Running Commands
Support
admin
Undo
Back
Continue
Activate Windows
Go to Settings to activate Windows.

Add Ranger KMS Service to Cluster 1

Review Changes

Ranger KMS Authentication Type hadoop.kms.authentication.type	Ranger KMS (Service-Wide) ○ simple ● kerberos
Ranger KMS Load Balancer ranger_kms_load_balancer	Ranger KMS (Service-Wide)
Ranger KMS Master Key Password ranger.db.encrypt.key.password	Ranger KMS Server Default Group ••••••••
Enable TLS/SSL for Ranger KMS Server ranger.service.https.attrib.ssl.enabled	☑ Ranger KMS Server Default Group
Ranger KMS Server TLS/SSL Server JKS Keystore File Location ranger.service.https.attrib.keystore.file	Ranger KMS Server Default Group {{CM_AUTO_TLS}}
Ranger KMS Server TLS/SSL Server JKS Keystore File Password ranger.service.https.attrib.keystore.pass	Ranger KMS Server Default Group ••••••
Ranger KMS Server TLS/SSL Client Trust Store File xasecure.policymgr.clientssl.truststore	Ranger KMS Server Default Group {{CM_AUTO_TLS}}
Ranger KMS Server TLS/SSL Client Trust Store Password xasecure.policymgr.clientssl.truststore.password	Ranger KMS Server Default Group ••••••

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**.



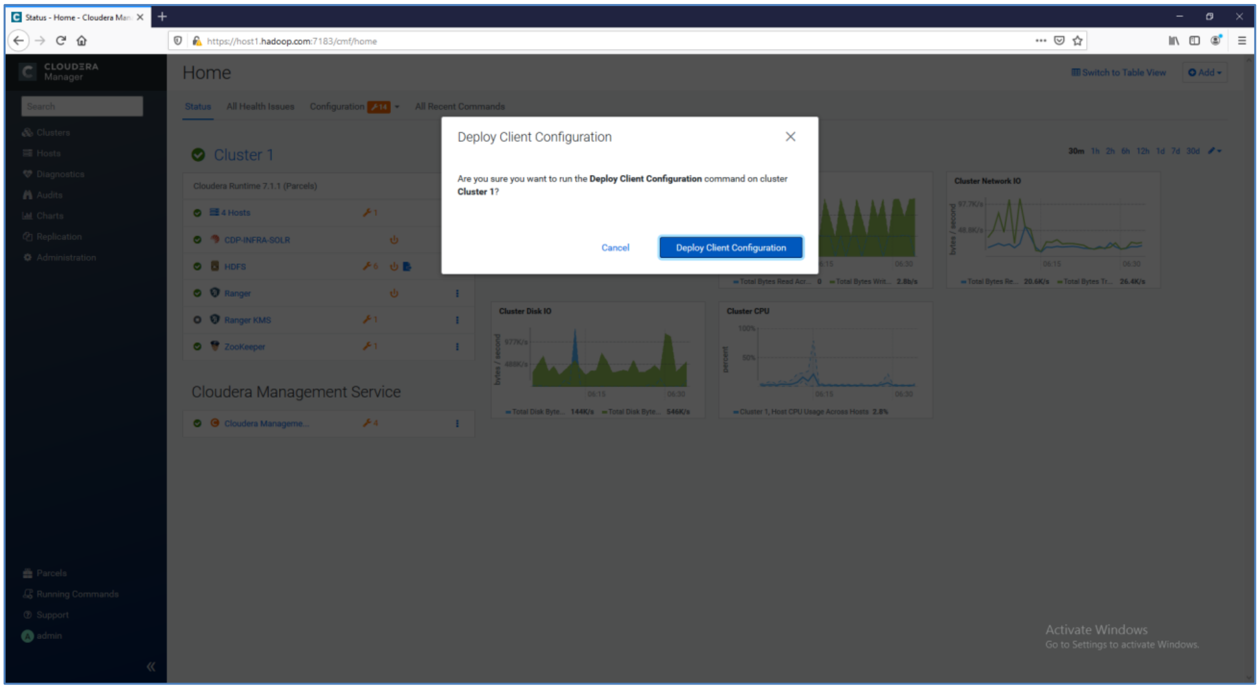
Add Ranger KMS Service to Cluster 1

Summary

Your new service is installed and configured on your cluster.

Note: You may still have to start your new service. It is recommended that you restart any dependency services with outdated configurations before doing so. You can perform these actions on the main page by clicking **Finish** below.

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.

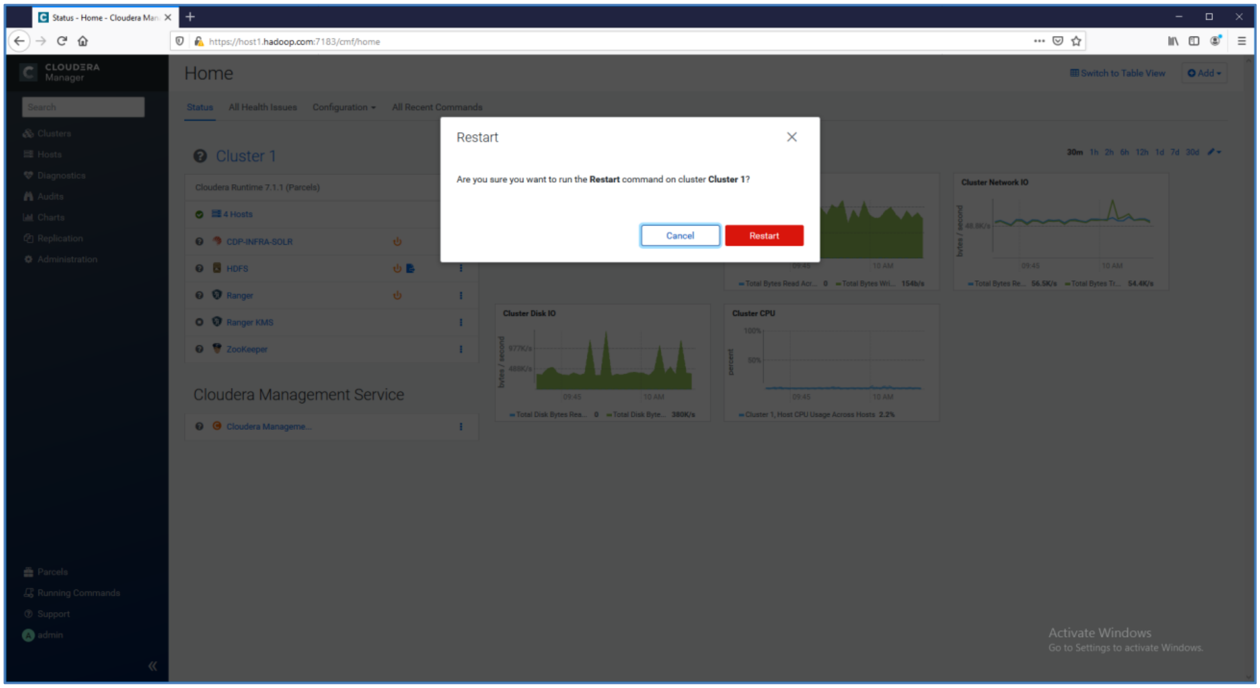


Deploy Client Configuration

Are you sure you want to run the **Deploy Client Configuration** command on cluster **Cluster 1**?

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

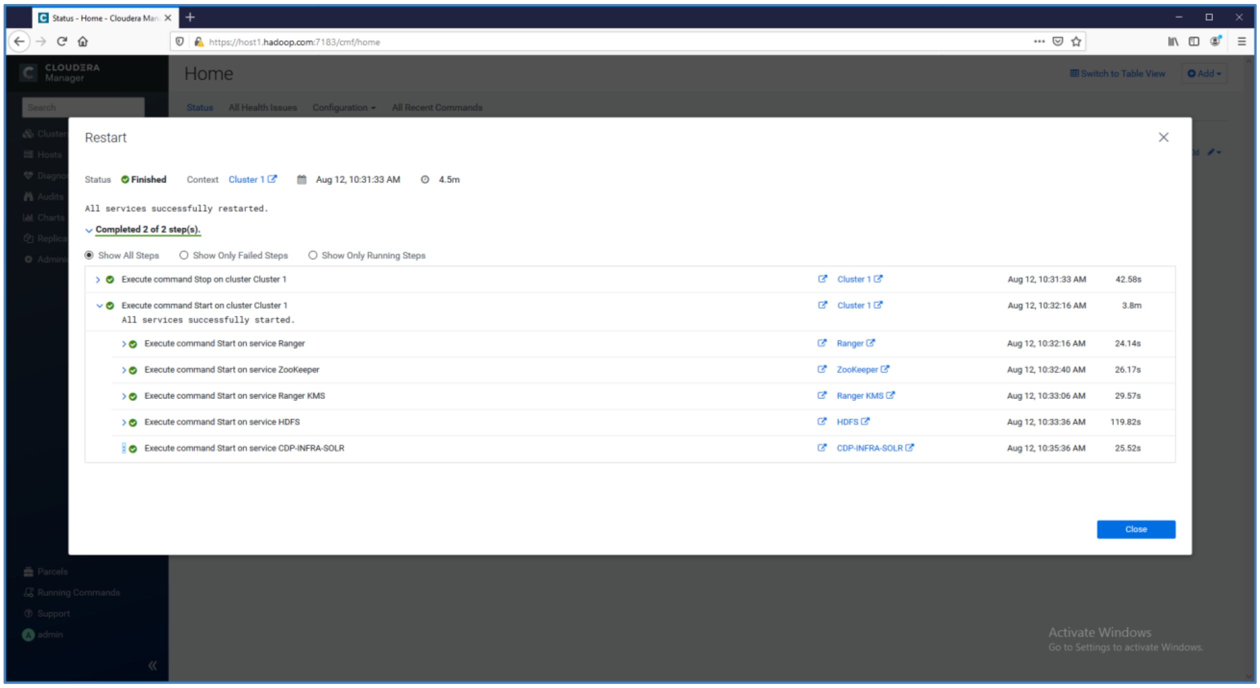
15. On the cluster **Home** page, click the More Options icon (•••) and then click **Restart**. Click the **Restart** again when the confirmation window pops up.



Restart

Are you sure you want to run the **Restart** command on cluster **Cluster 1**?

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



Restart

Status ✓ Finished   Context Cluster 1   Aug 12, 10:31:33 AM   4.5m

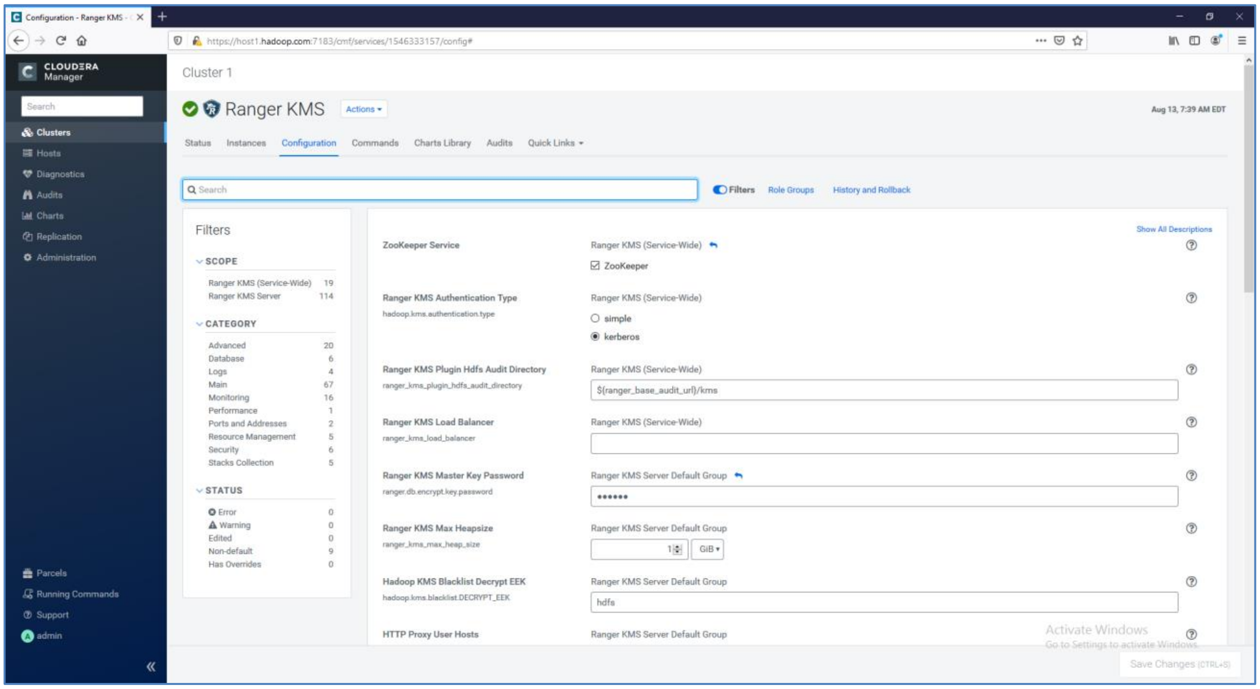
```
All services successfully restarted.
```

Completed 2 of 2 step(s).

● Show All Steps   ○ Show Only Failed Steps   ○ Show Only Running Steps

Execute command Stop on cluster Cluster 1	Cluster 1	Aug 12, 10:31:33 AM	42.58s
Execute command Start on cluster Cluster 1 All services successfully started.	Cluster 1	Aug 12, 10:32:16 AM	3.8m
Execute command Start on service Ranger	Ranger	Aug 12, 10:32:16 AM	24.14s
Execute command Start on service ZooKeeper	ZooKeeper	Aug 12, 10:32:40 AM	26.17s
Execute command Start on service Ranger KMS	Ranger KMS	Aug 12, 10:33:06 AM	29.57s
Execute command Start on service HDFS	HDFS	Aug 12, 10:33:36 AM	119.82s
Execute command Start on service CDP-INFRA-SOLR	CDP-INFRA-SOLR	Aug 12, 10:35:36 AM	25.52s

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



ZooKeeper Service — Ranger KMS (Service-Wide) — ☑ ZooKeeper

Ranger KMS Authentication Type (hadoop.kms.authentication.type) — Ranger KMS (Service-Wide) — ○ simple ● kerberos

Ranger KMS Plugin Hdfs Audit Directory (ranger_kms_plugin_hdfs_audit_directory) — Ranger KMS (Service-Wide) — ${ranger_base_audit_url}/kms

Ranger KMS Load Balancer (ranger_kms_load_balancer) — Ranger KMS (Service-Wide)

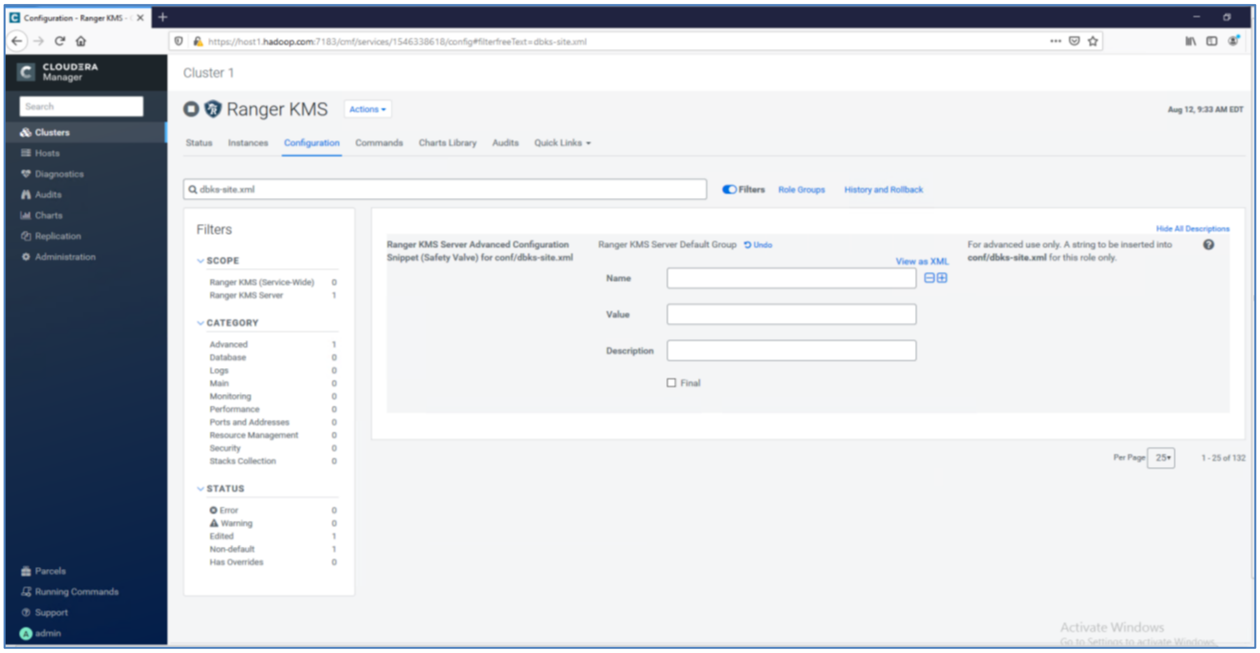
Ranger KMS Master Key Password (ranger.db.encrypt.key.password) — Ranger KMS Server Default Group — ••••••

Ranger KMS Max Heapsize (ranger_kms_max_heap_size) — Ranger KMS Server Default Group — 1 GiB

Hadoop KMS Blacklist Decrypt EEK (hadoop.kms.blacklist.DECRYPT_EEK) — Ranger KMS Server Default Group — hdfs

HTTP Proxy User Hosts — Ranger KMS Server Default Group

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.**



Search: dbks-site.xml

Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml — Ranger KMS Server Default Group

Name:

Value:

Description:

□ Final

For advanced use only. A string to be inserted into **conf/dbks-site.xml** for this role only.

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`

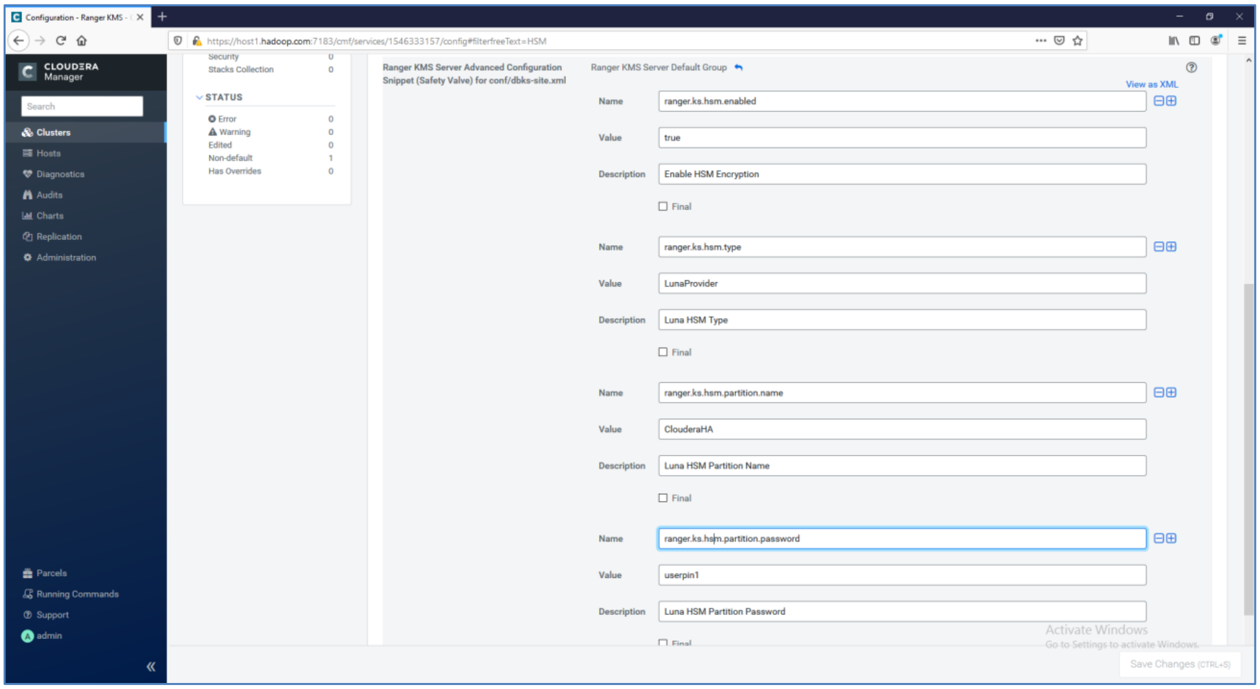
Description: `Luna HSM Partition Name`

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)**.



Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml

Ranger KMS Server Default Group

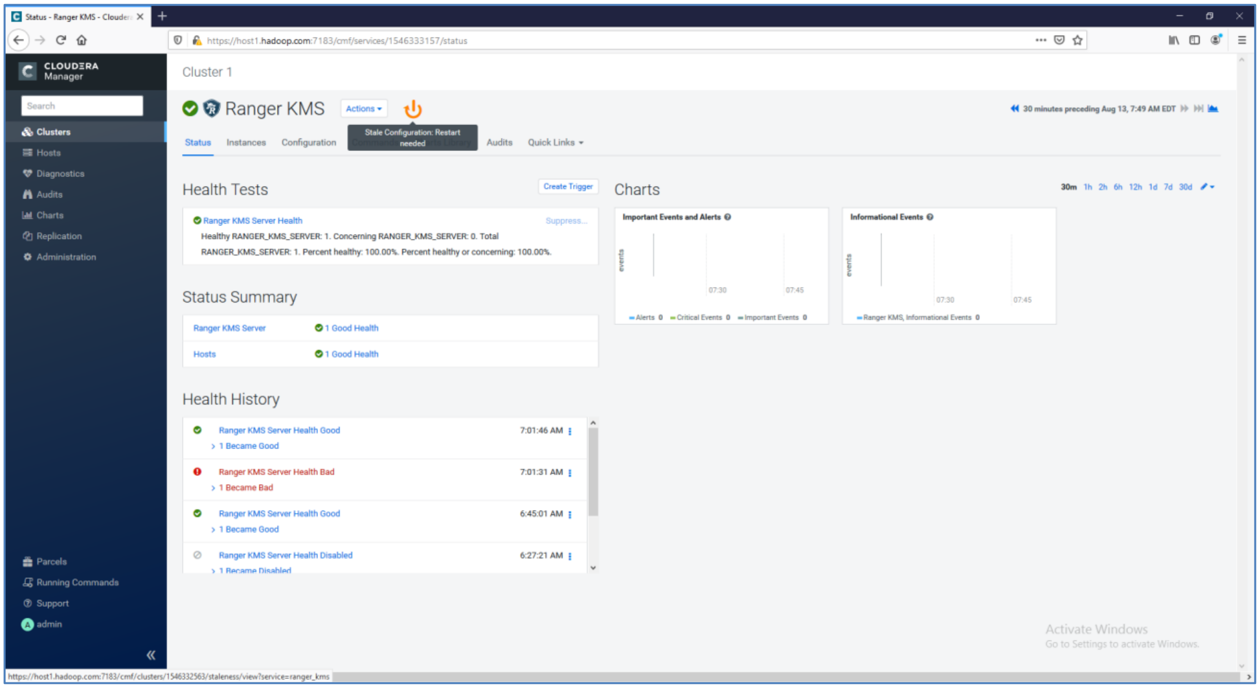
Name: ranger.ks.hsm.enabled
Value: true
Description: Enable HSM Encryption
□ Final

Name: ranger.ks.hsm.type
Value: LunaProvider
Description: Luna HSM Type
□ Final

Name: ranger.ks.hsm.partition.name
Value: ClouderaHA
Description: Luna HSM Partition Name
□ Final

Name: ranger.ks.hsm.partition.password
Value: userpin1
Description: Luna HSM Partition Password
□ Final

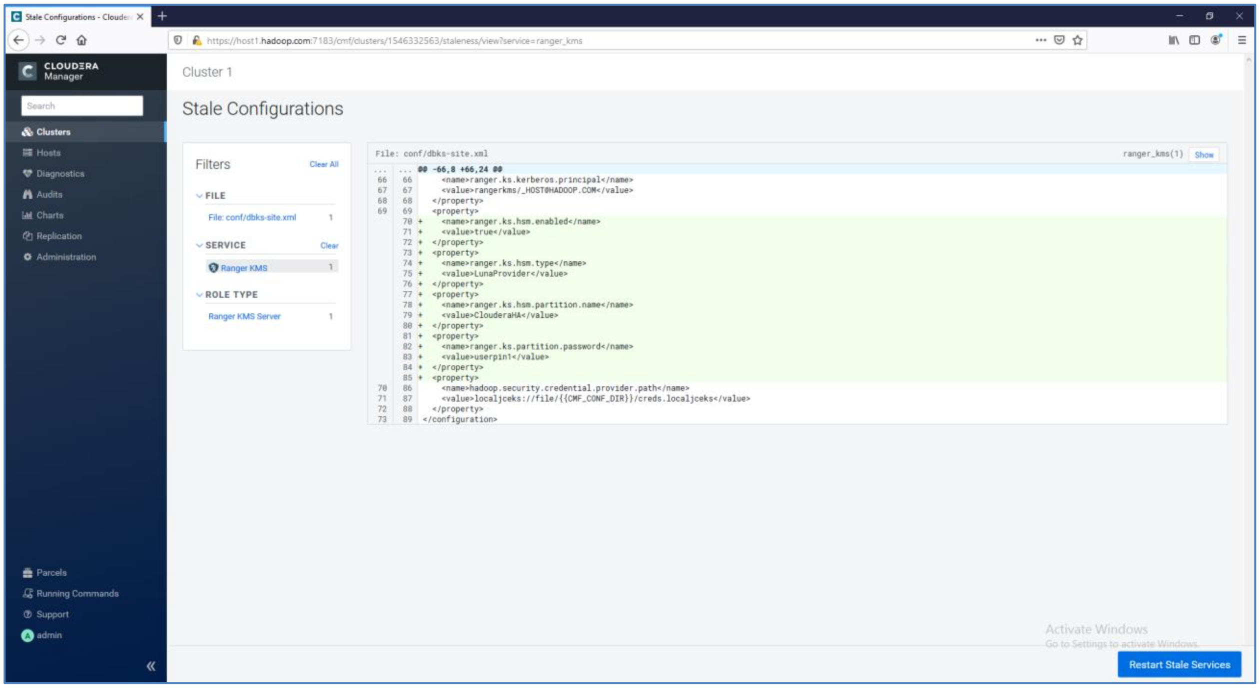
20. After the changes are saved, click on Cloudera Manager icon in the left pane to go back to Cluster Home page. Click **Ranger KMS** service and then click the restart icon to restart the service.



Healthy RANGER_KMS_SERVER: 1. Concerning RANGER_KMS_SERVER: 0. Total RANGER_KMS_SERVER: 1. Percent healthy: 100.00%. Percent healthy or concerning: 100.00%.

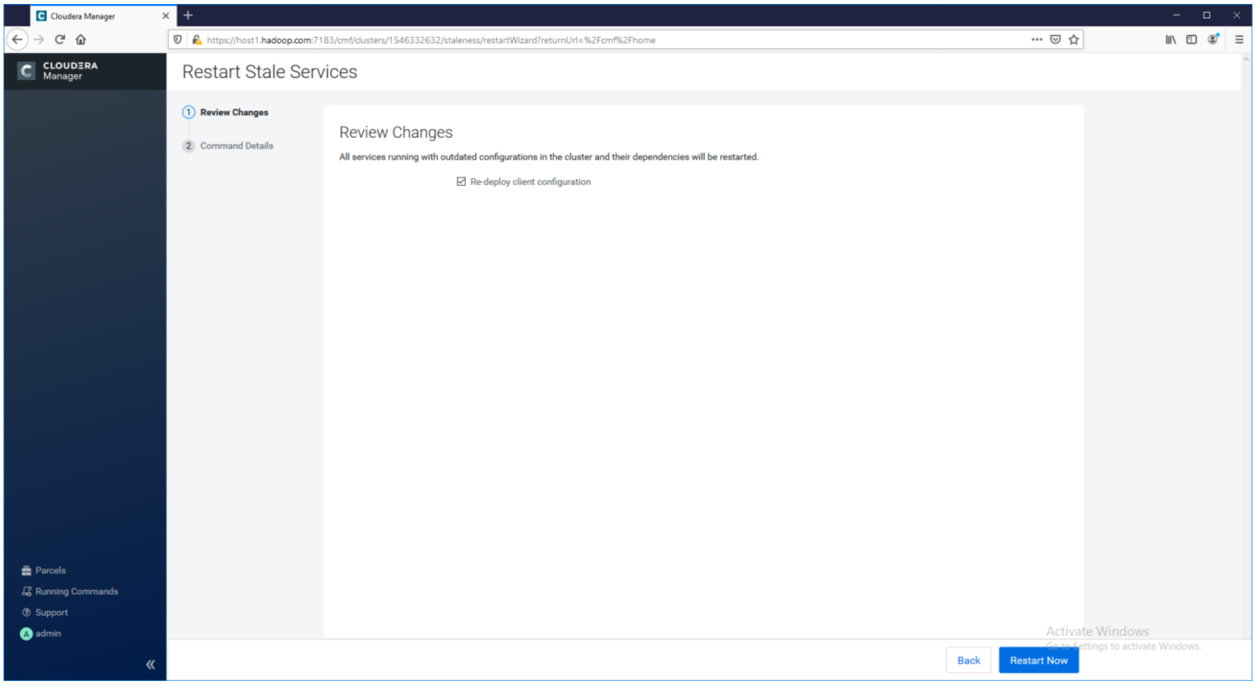
NOTE: Ensure that kms user is added to the hsmusers group.

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



```
File: conf/dbks-site.xml
@@ -66,8 +66,24 @@
      <name>ranger.ks.kerberos.principal</name>
      <value>rangerkms/_HOST@HADOOP.COM</value>
    </property>
    <property>
+     <name>ranger.ks.hsm.enabled</name>
+     <value>true</value>
+   </property>
+   <property>
+     <name>ranger.ks.hsm.type</name>
+     <value>LunaProvider</value>
+   </property>
+   <property>
+     <name>ranger.ks.hsm.partition.name</name>
+     <value>ClouderaHA</value>
+   </property>
+   <property>
+     <name>ranger.ks.partition.password</name>
+     <value>userpin1</value>
+   </property>
+   <property>
      <name>hadoop.security.credential.provider.path</name>
      <value>localjceks://file/{{CMF_CONF_DIR}}/creds.localjceks</value>
    </property>
  </configuration>
```

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


Cloudera Manager
https://host1.hadoop.com:7183/cmf/clusters/1546332632/staleness/restartWizard?returnUrl=%2Fcmf%2Fhome
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Activate Windows
Go to Settings to activate Windows.

Restart Stale Services

1 Review Changes

2 Command Details

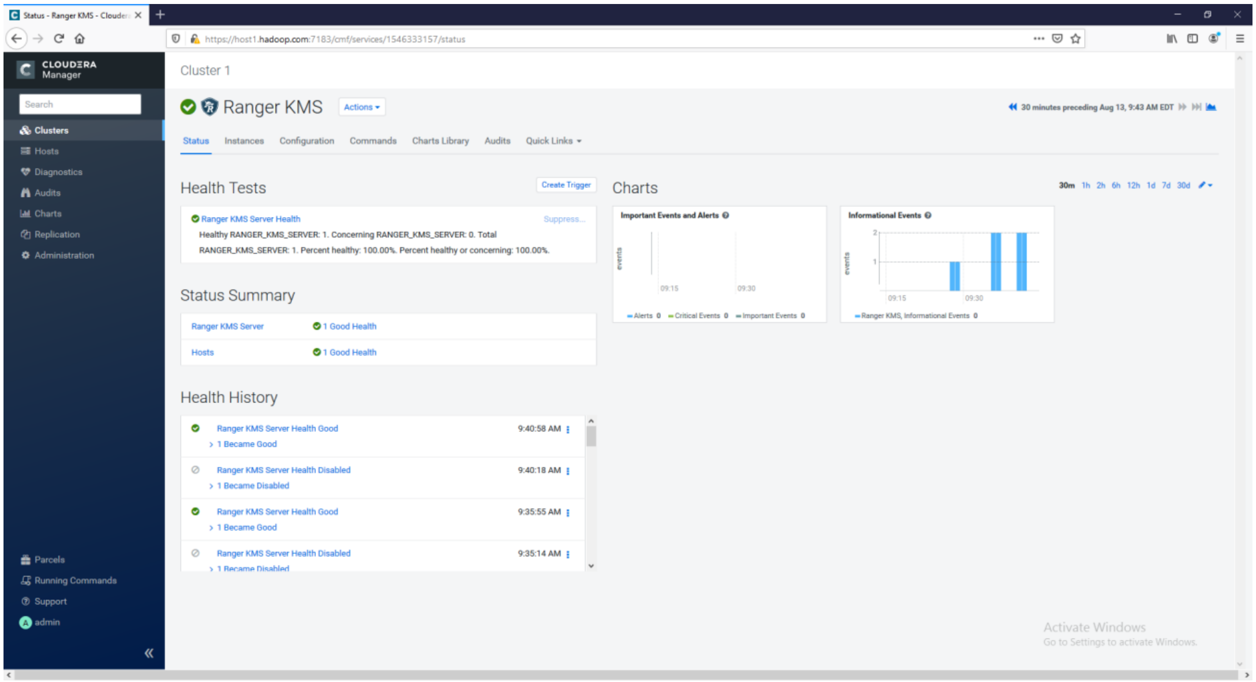
Review Changes

All services running with outdated configurations in the cluster and their dependencies will be restarted.

☑ Re-deploy client configuration

Back | Restart Now

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



Cluster 1

Ranger KMS

30 minutes preceding Aug 13, 9:43 AM EDT

Health Tests

✓ Ranger KMS Server Health

Healthy RANGER_KMS_SERVER: 1. Concerning RANGER_KMS_SERVER: 0. Total RANGER_KMS_SERVER: 1. Percent healthy: 100.00%. Percent healthy or concerning: 100.00%.

Charts

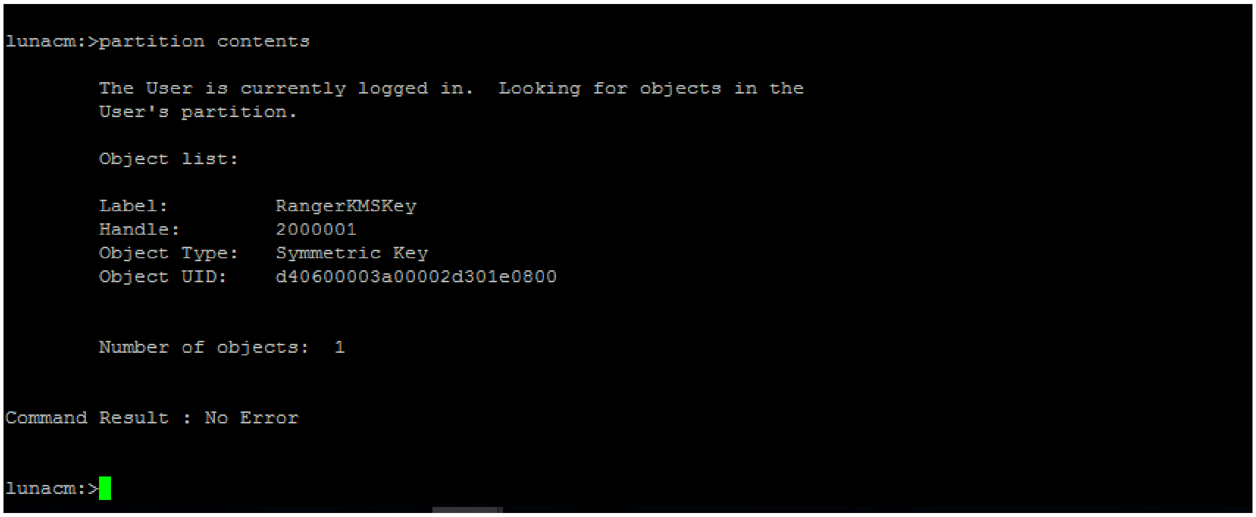
Status Summary

Ranger KMS Server	✓ 1 Good Health
Hosts	✓ 1 Good Health

Health History

✓	Ranger KMS Server Health Good › 1 Became Good	9:40:58 AM
⊘	Ranger KMS Server Health Disabled › 1 Became Disabled	9:40:18 AM
✓	Ranger KMS Server Health Good › 1 Became Good	9:35:55 AM
⊘	Ranger KMS Server Health Disabled › 1 Became Disabled	9:35:14 AM

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



```
lunacm:>partition contents

        The User is currently logged in.  Looking for objects in the
        User's partition.

        Object list:

        Label:          RangerKMSKey
        Handle:         2000001
        Object Type:    Symmetric Key
        Object UID:     d40600003a00002d301e0800


        Number of objects:  1

Command Result : No Error

lunacm:>
```

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`

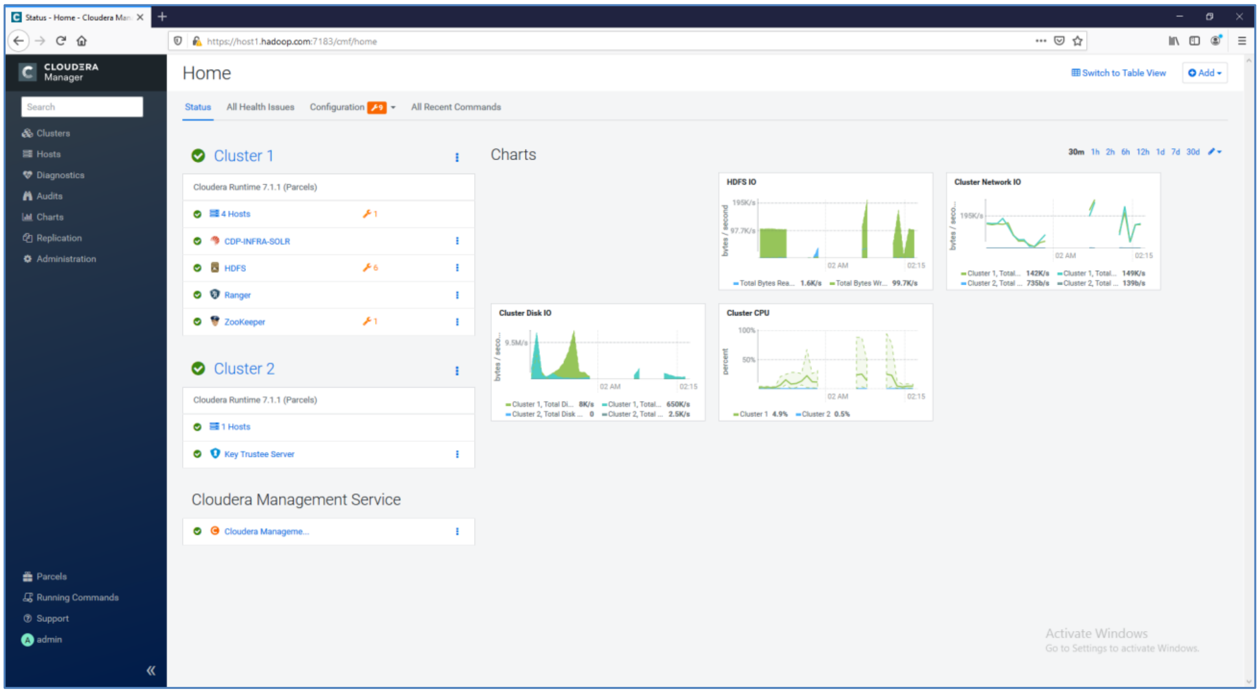
   Password: `admin`

   > **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.

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

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.

```
# 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
--------------------------------------------------------------------------
```

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]10.164.78.79
Will attempt to setup listener on 10.164.78.79
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 : 10.164.78.79

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

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

> **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.

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 Error! Hyperlink reference not valid. hostname or ip>: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://host5.hadoop.com: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://host5.hadoop.com: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:

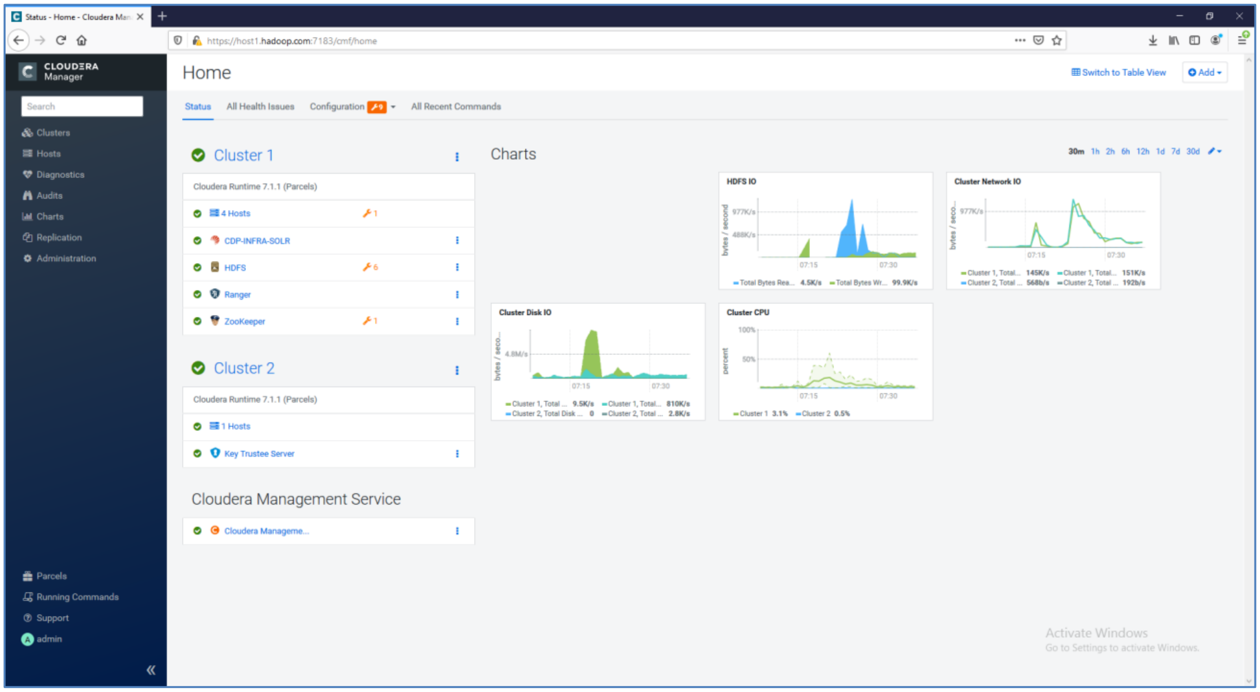
    ```
    ----------------------------------------------------------------------------------------------------------------------------------
    "Sample Key TEST_HELLO_DEPOSIT2020-09-01-134034 has been created"
    ---------------------------------------------------------------------------
    ```

    > **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.

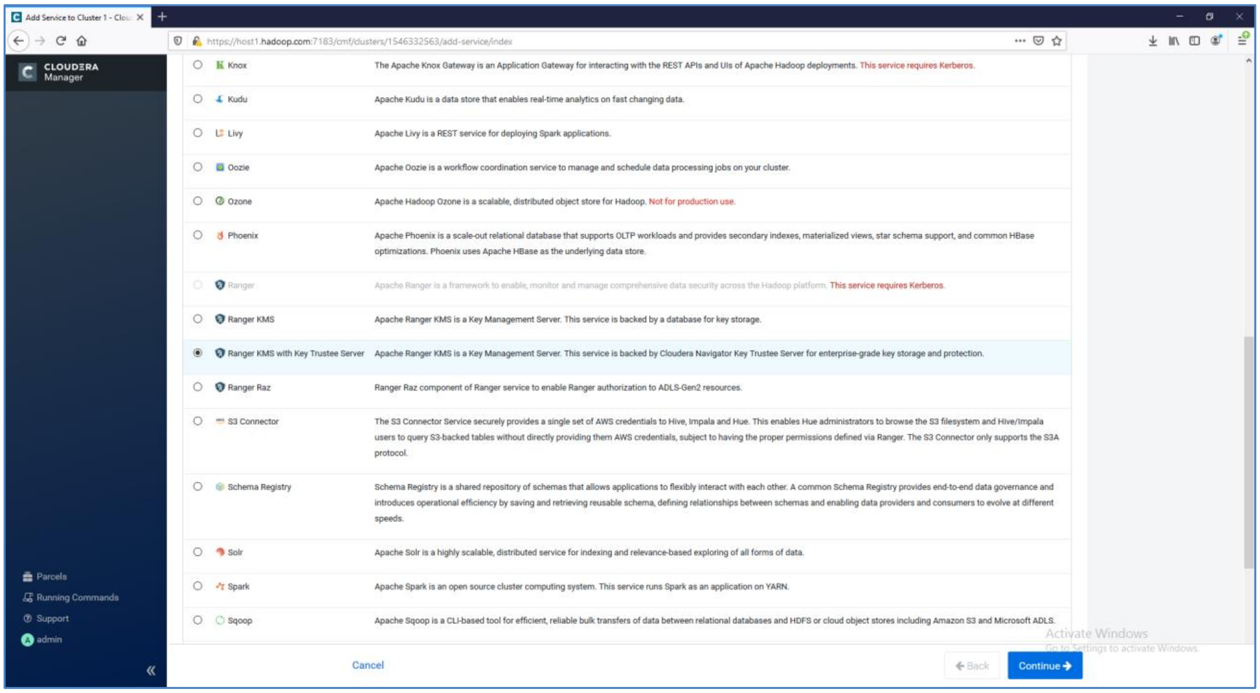
13. Before you begin the installation on **Ranger KMS with Key Trustee Server**, ensure that:

    - 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**.



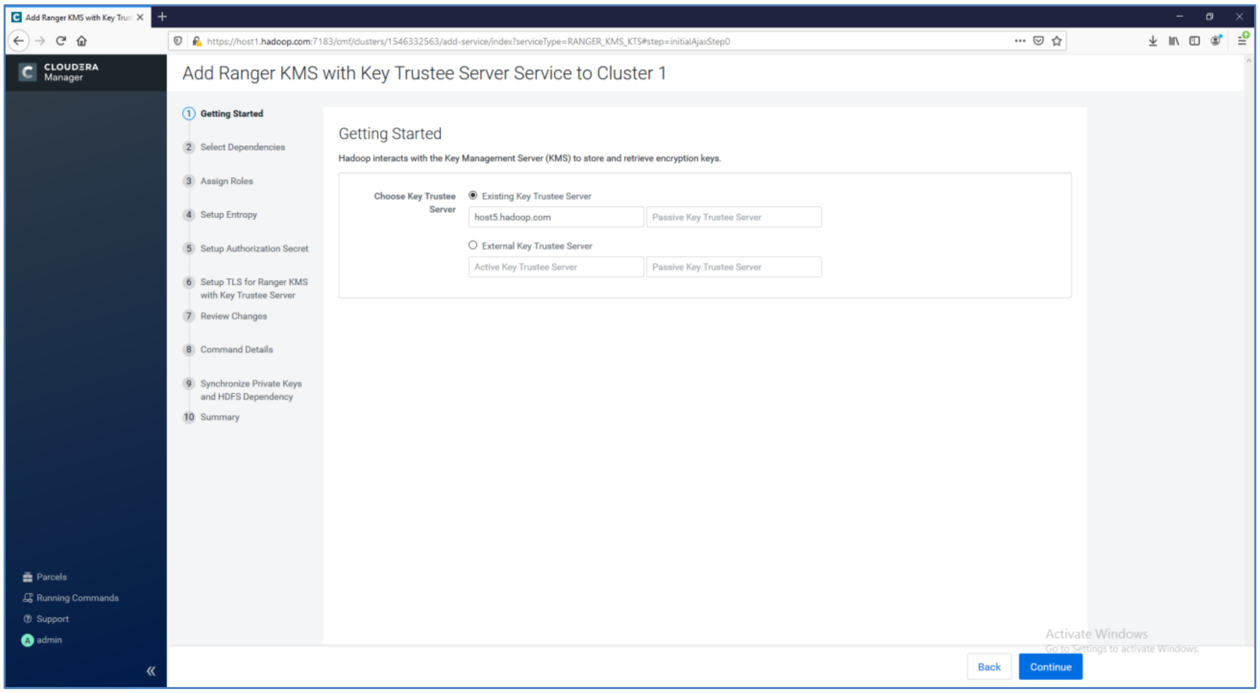
14. Select **Ranger KMS with Key Trustee Server** and click **Continue**.


Add Service to Cluster 1 - Clou
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Cancel
Back
Continue
Activate Windows
Go to Settings to activate Windows.

○	Knox	The Apache Knox Gateway is an Application Gateway for interacting with the REST APIs and UIs of Apache Hadoop deployments. This service requires Kerberos.
○	Kudu	Apache Kudu is a data store that enables real-time analytics on fast changing data.
○	Livy	Apache Livy is a REST service for deploying Spark applications.
○	Oozie	Apache Oozie is a workflow coordination service to manage and schedule data processing jobs on your cluster.
○	Ozone	Apache Hadoop Ozone is a scalable, distributed object store for Hadoop. Not for production use.
○	Phoenix	Apache Phoenix is a scale-out relational database that supports OLTP workloads and provides secondary indexes, materialized views, star schema support, and common HBase optimizations. Phoenix uses Apache HBase as the underlying data store.
○	Ranger	Apache Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform. This service requires Kerberos.
○	Ranger KMS	Apache Ranger KMS is a Key Management Server. This service is backed by a database for key storage.
●	Ranger KMS with Key Trustee Server	Apache Ranger KMS is a Key Management Server. This service is backed by Cloudera Navigator Key Trustee Server for enterprise-grade key storage and protection.
○	Ranger Raz	Ranger Raz component of Ranger service to enable Ranger authorization to ADLS-Gen2 resources.
○	S3 Connector	The S3 Connector Service securely provides a single set of AWS credentials to Hive, Impala and Hue. This enables Hue administrators to browse the S3 filesystem and Hive/Impala users to query S3-backed tables without directly providing them AWS credentials, subject to having the proper permissions defined via Ranger. The S3 Connector only supports the S3A protocol.
○	Schema Registry	Schema Registry is a shared repository of schemas that allows applications to flexibly interact with each other. A common Schema Registry provides end-to-end data governance and introduces operational efficiency by saving and retrieving reusable schema, defining relationships between schemas and enabling data providers and consumers to evolve at different speeds.
○	Solr	Apache Solr is a highly scalable, distributed service for indexing and relevance-based exploring of all forms of data.
○	Spark	Apache Spark is an open source cluster computing system. This service runs Spark as an application on YARN.
○	Sqoop	Apache Sqoop is a CLI-based tool for efficient, reliable bulk transfers of data between relational databases and HDFS or cloud object stores including Amazon S3 and Microsoft ADLS.

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**.


Add Ranger KMS with Key Trus
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=initialAjaxStep0
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Back
Continue
Activate Windows
Go to Settings to activate Windows.

Add Ranger KMS with Key Trustee Server Service to Cluster 1

1. Getting Started
2. Select Dependencies
3. Assign Roles
4. Setup Entropy
5. Setup Authorization Secret
6. Setup TLS for Ranger KMS with Key Trustee Server
7. Review Changes
8. Command Details
9. Synchronize Private Keys and HDFS Dependency
10. Summary

Getting Started

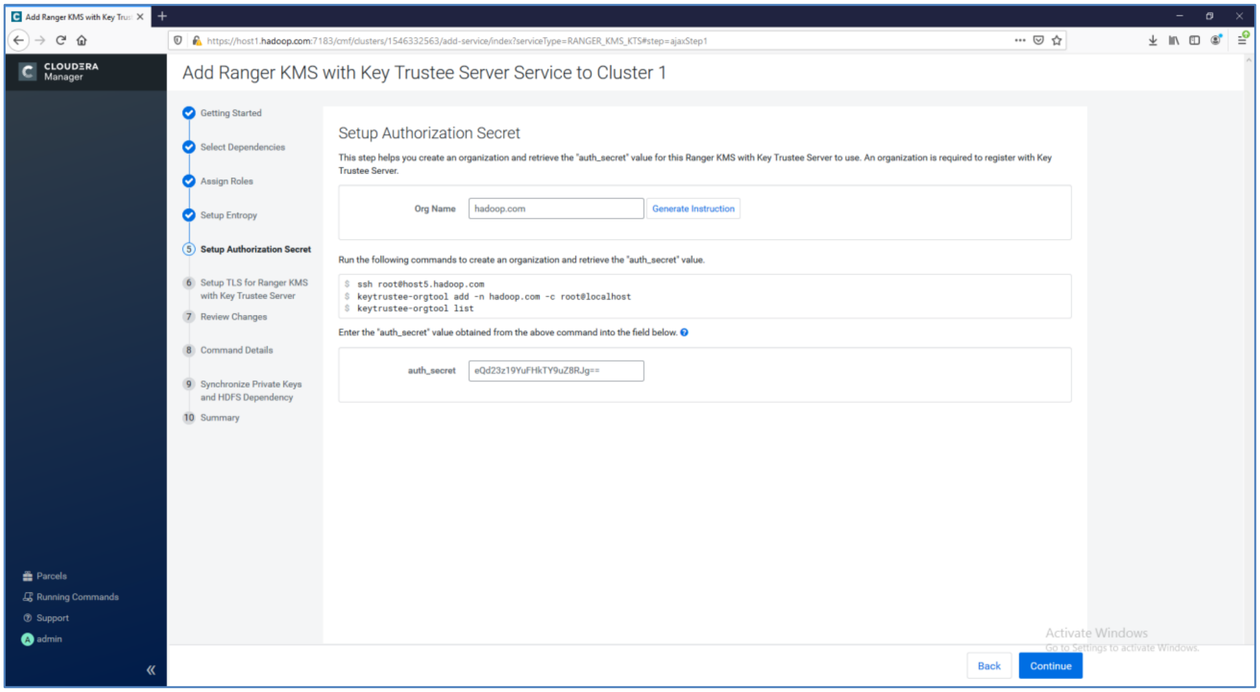
Hadoop interacts with the Key Management Server (KMS) to store and retrieve encryption keys.

Choose Key Trustee Server
● Existing Key Trustee Server
host5.hadoop.com | Passive Key Trustee Server
○ External Key Trustee Server
Active Key Trustee Server | Passive Key Trustee Server

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**.


Add Ranger KMS with Key Trus
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=ajaxStep1
CLOUDERA Manager
Add Ranger KMS with Key Trustee Server Service to Cluster 1
Getting Started
Select Dependencies
Assign Roles
Setup Entropy
5 Setup Authorization Secret
6 Setup TLS for Ranger KMS with Key Trustee Server
7 Review Changes
8 Command Details
9 Synchronize Private Keys and HDFS Dependency
10 Summary
Parcels
Running Commands
Support
admin
Activate Windows
Go to Settings to activate Windows.
Back
Continue

Setup Authorization Secret

This step helps you create an organization and retrieve the "auth_secret" value for this Ranger KMS with Key Trustee Server to use. An organization is required to register with Key Trustee Server.

Org Name: hadoop.com   Generate Instruction

Run the following commands to create an organization and retrieve the "auth_secret" value.

```
$ ssh root@host5.hadoop.com
$ keytrustee-orgtool add -n hadoop.com -c root@localhost
$ keytrustee-orgtool list
```

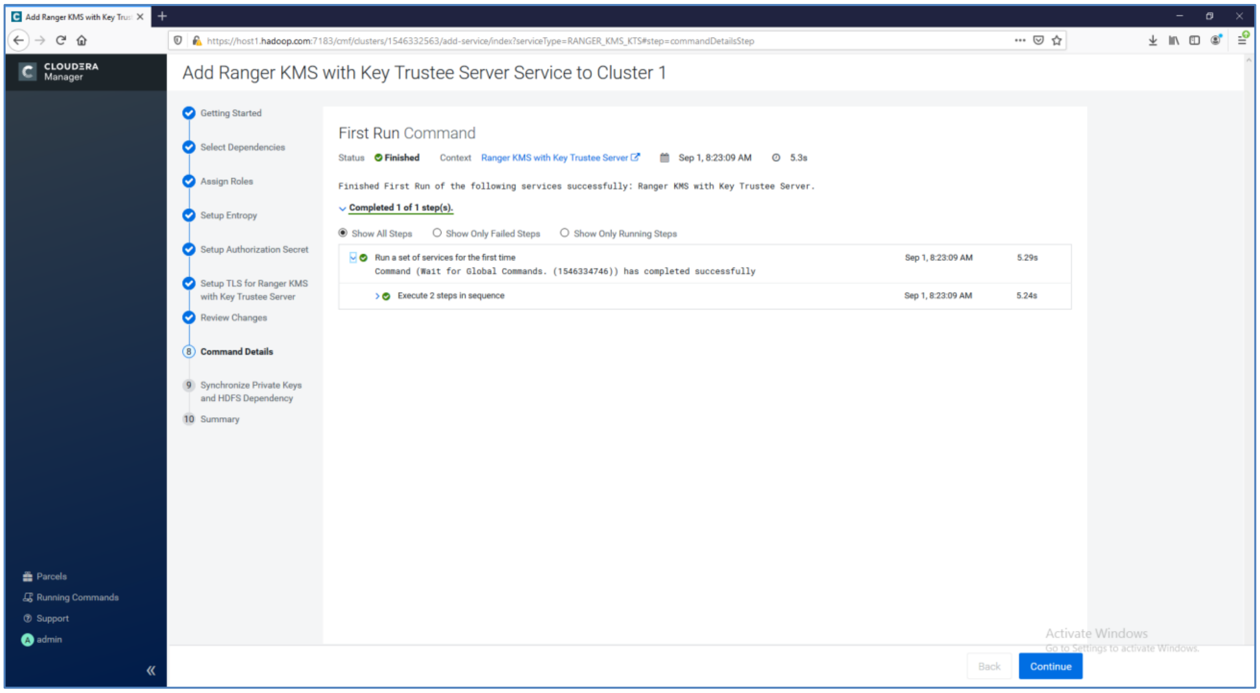
Enter the "auth_secret" value obtained from the above command into the field below.

auth_secret: eQd23z19YuFHkTY9uZ8RJg==

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.


Add Ranger KMS with Key Trus
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=commandDetailsStep
CLOUDERA Manager
Add Ranger KMS with Key Trustee Server Service to Cluster 1
Getting Started
Select Dependencies
Assign Roles
Setup Entropy
Setup Authorization Secret
Setup TLS for Ranger KMS with Key Trustee Server
Review Changes
8 Command Details
9 Synchronize Private Keys and HDFS Dependency
10 Summary
Parcels
Running Commands
Support
admin
Activate Windows
Go to Settings to activate Windows.
Back
Continue

First Run Command

Status: Finished   Context: Ranger KMS with Key Trustee Server   Sep 1, 8:23:09 AM   5.3s

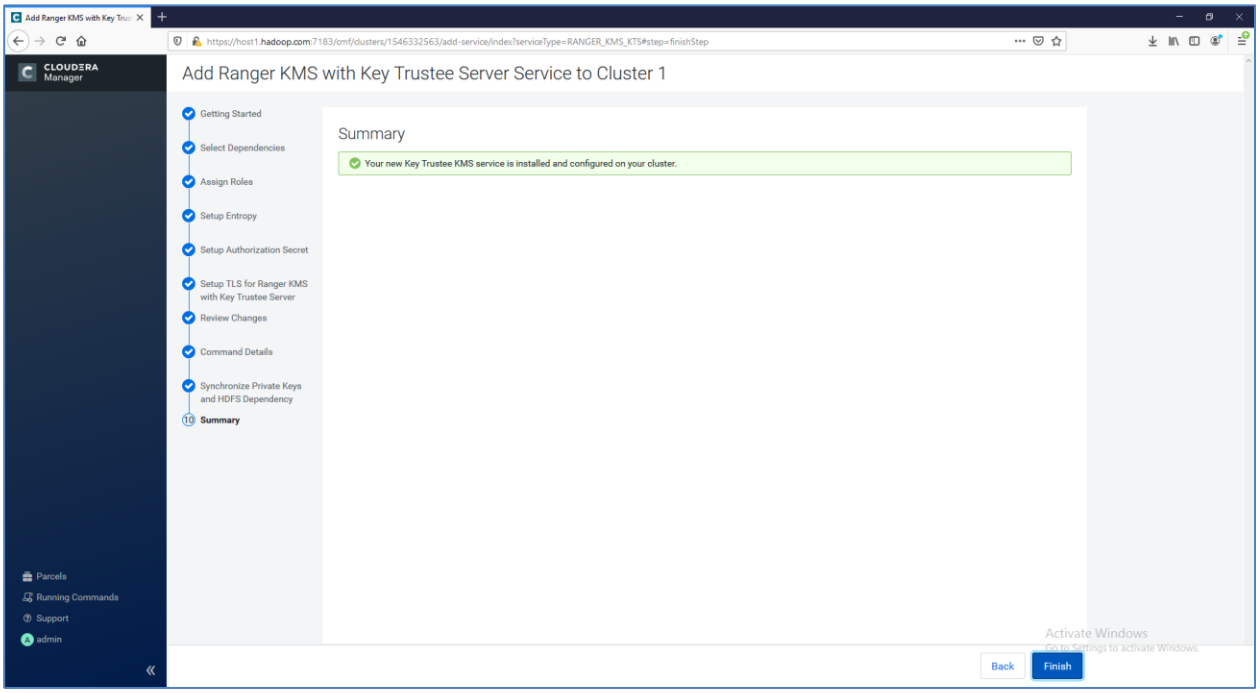
```
Finished First Run of the following services successfully: Ranger KMS with Key Trustee Server.
```

Completed 1 of 1 step(s).

● Show All Steps ○ Show Only Failed Steps ○ Show Only Running Steps

Run a set of services for the first time `Command (Wait for Global Commands. (1546334746)) has completed successfully`	Sep 1, 8:23:09 AM	5.29s
Execute 2 steps in sequence	Sep 1, 8:23:09 AM	5.24s

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



Add Ranger KMS with Key Trustee Server Service to Cluster 1

- Getting Started
- Select Dependencies
- Assign Roles
- Setup Entropy
- Setup Authorization Secret
- Setup TLS for Ranger KMS with Key Trustee Server
- Review Changes
- Command Details
- Synchronize Private Keys and HDFS Dependency
- 10 Summary

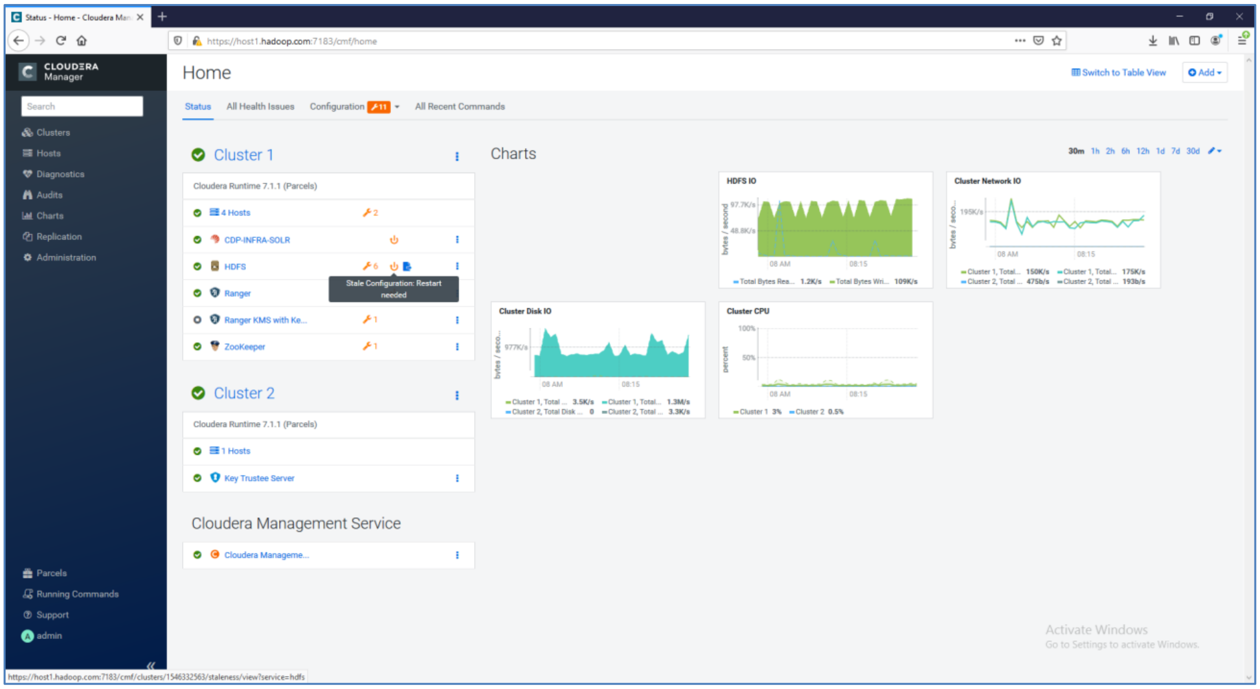
Summary

Your new Key Trustee KMS service is installed and configured on your cluster.

Add Ranger KMS with Key Trus
https://host1.hadoop.com:7183/cmf/clusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=finishStep
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Activate Windows
Go to Settings to activate Windows.
Back
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**.



Home

Cluster 1

Cloudera Runtime 7.1.1 (Parcels)

- 4 Hosts 2
- CDP-INFRA-SOLR
- HDFS 6
- Ranger
- Ranger KMS with Ke... 1
- ZooKeeper 1

Stale Configuration: Restart needed

Cluster 2

Cloudera Runtime 7.1.1 (Parcels)

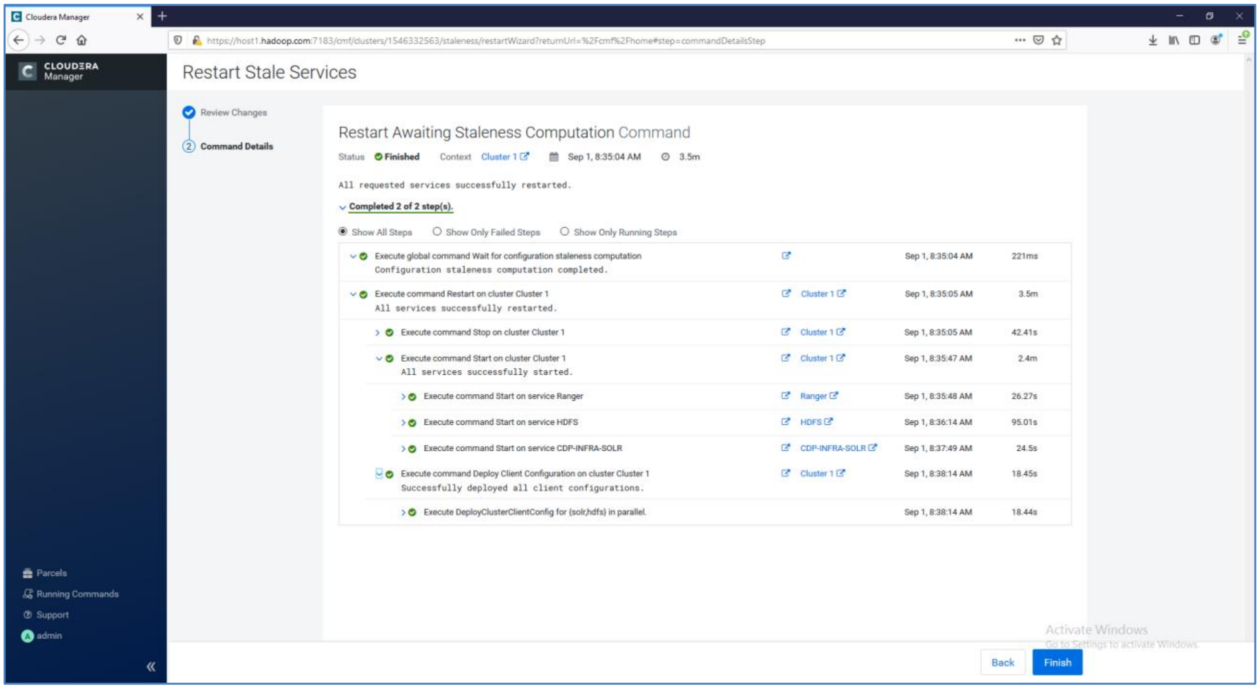
- 1 Hosts
- Key Trustee Server

Cloudera Management Service

- Cloudera Manageme...

https://host1.hadoop.com:7183/cmf/clusters/1546332563/staleness/view?service=hdfs

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



Restart Stale Services

✓ Review Changes

(2) Command Details

Restart Awaiting Staleness Computation Command

Status ✓ Finished Context Cluster 1 Sep 1, 8:35:04 AM 3.5m

```
All requested services successfully restarted.
```

Completed 2 of 2 step(s).

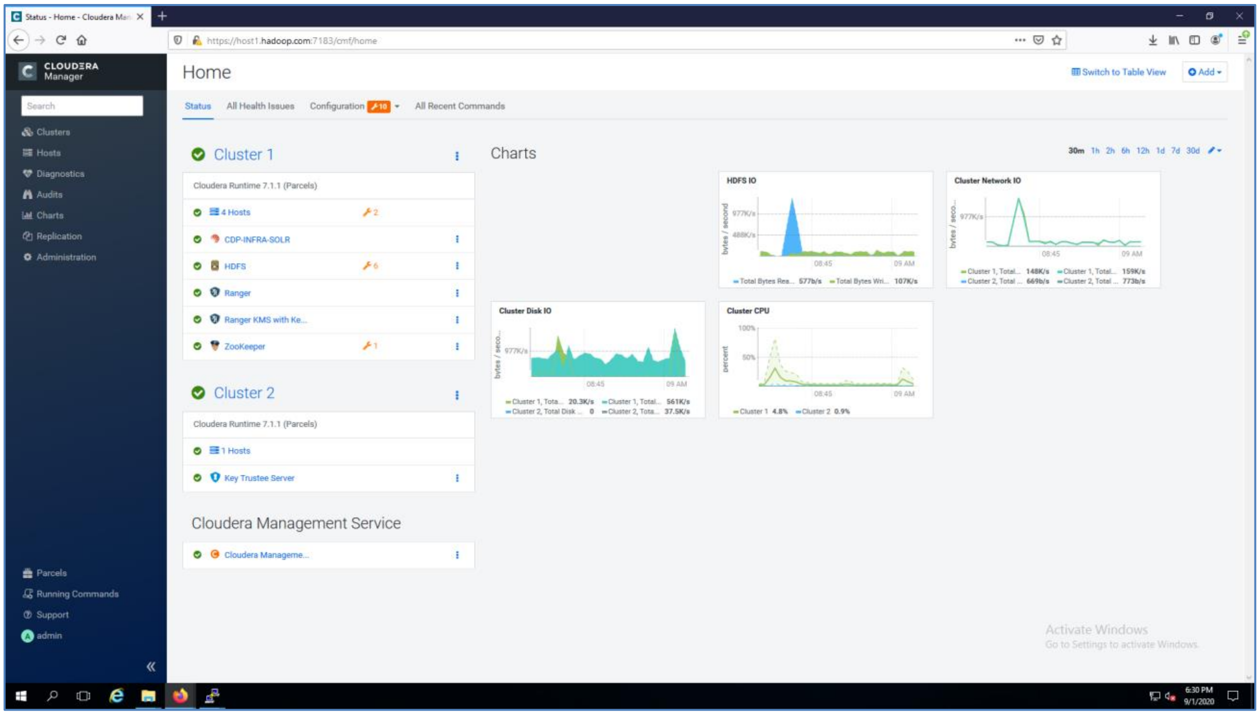
● Show All Steps ○ Show Only Failed Steps ○ Show Only Running Steps

Step	Context	Start time	Duration
Execute global command Wait for configuration staleness computation Configuration staleness computation completed.		Sep 1, 8:35:04 AM	221ms
Execute command Restart on cluster Cluster 1 All services successfully restarted.	Cluster 1	Sep 1, 8:35:05 AM	3.5m
Execute command Stop on cluster Cluster 1	Cluster 1	Sep 1, 8:35:05 AM	42.41s
Execute command Start on cluster Cluster 1 All services successfully started.	Cluster 1	Sep 1, 8:35:47 AM	2.4m
Execute command Start on service Ranger	Ranger	Sep 1, 8:35:48 AM	26.27s
Execute command Start on service HDFS	HDFS	Sep 1, 8:36:14 AM	95.01s
Execute command Start on service CDP-INFRA-SOLR	CDP-INFRA-SOLR	Sep 1, 8:37:49 AM	24.5s
Execute command Deploy Client Configuration on cluster Cluster 1 Successfully deployed all client configurations.	Cluster 1	Sep 1, 8:38:14 AM	18.45s
Execute DeployClusterClientConfig for (solr,hdfs) in parallel.		Sep 1, 8:38:14 AM	18.44s

Cloudera Manager
https://host1.hadoop.com:7183/cmf/clusters/1546332563/staleness/restartWizard?returnUrl=%2Fcmf%2Fhome#step=commandDetailsStep
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Back
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.



Home

Status All Health Issues Configuration 10 All Recent Commands

Cluster 1

Cloudera Runtime 7.1.1 (Parcels)

- ✓ 4 Hosts 2
- ✓ CDP-INFRA-SOLR
- ✓ HDFS 6
- ✓ Ranger
- ✓ Ranger KMS with Ke...
- ✓ ZooKeeper 1

Cluster 2

Cloudera Runtime 7.1.1 (Parcels)

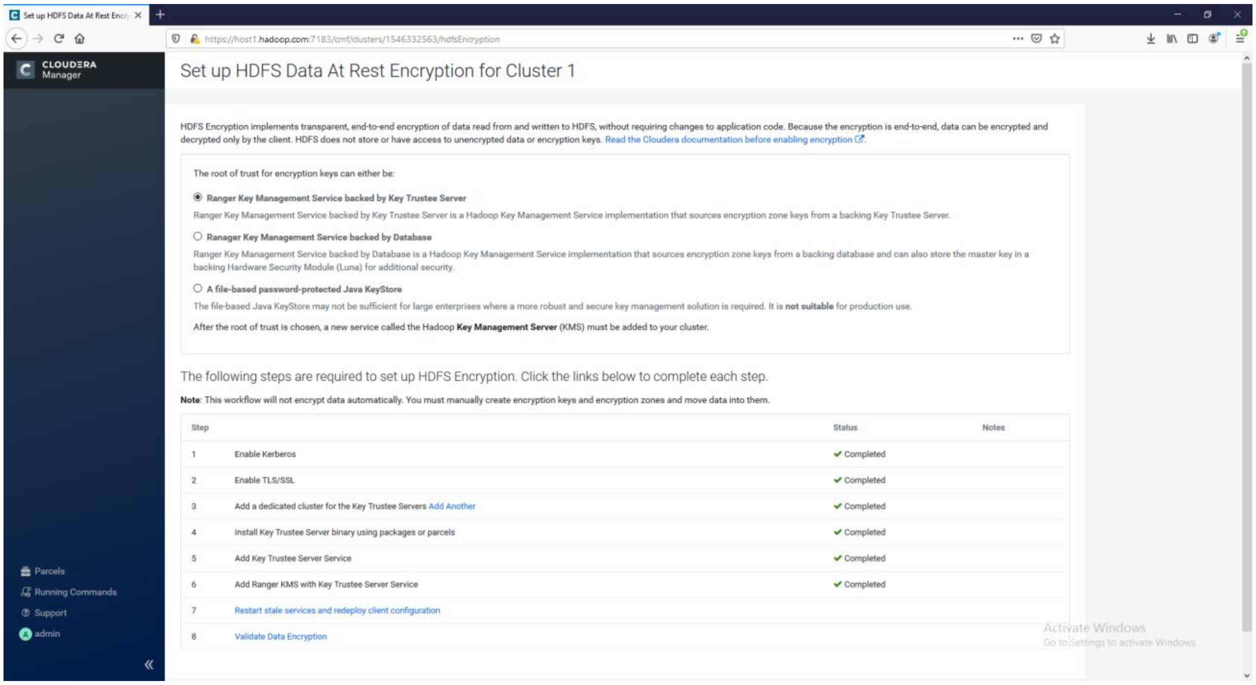
- ✓ 1 Hosts
- ✓ Key Trustee Server

Cloudera Management Service

- ✓ Cloudera Manageme...

Status - Home - Cloudera Man
https://host1.hadoop.com:7183/cmf/home
CLOUDERA Manager
Search
Clusters
Hosts
Diagnostics
Audits
Charts
Replication
Administration
Parcels
Running Commands
Support
admin
Switch to Table View
Add
Charts
30m 1h 2h 6h 12h 1d 7d 30d
HDFS IO
Cluster Network IO
Cluster Disk IO
Cluster CPU
bytes / second
percent
977K/s
488K/s
100%
50%
08:45
09 AM
Total Bytes Rea... 577b/s
Total Bytes Wri... 107K/s
Cluster 1, Total... 148K/s
Cluster 1, Total... 159K/s
Cluster 2, Total... 669b/s
Cluster 2, Total... 773b/s
Cluster 1, Tota... 20.3K/s
Cluster 1, Total... 561K/s
Cluster 2, Total Disk... 0
Cluster 2, Tota... 37.5K/s
Cluster 1 4.8%
Cluster 2 0.9%
6:30 PM
9/1/2020

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.



Set up HDFS Data At Rest Encry
https://host1.hadoop.com:7183/cmf/clusters/1546332563/hdfsEncryption
CLOUDERA Manager
Parcels
Running Commands
Support
admin
Activate Windows
Go to Settings to activate Windows.

Set up HDFS Data At Rest Encryption for Cluster 1

HDFS Encryption implements transparent, end-to-end encryption of data read from and written to HDFS, without requiring changes to application code. Because the encryption is end-to-end, data can be encrypted and decrypted only by the client. HDFS does not store or have access to unencrypted data or encryption keys. Read the Cloudera documentation before enabling encryption.

The root of trust for encryption keys can either be:

● **Ranger Key Management Service backed by Key Trustee Server**
Ranger Key Management Service backed by Key Trustee Server is a Hadoop Key Management Service implementation that sources encryption zone keys from a backing Key Trustee Server.

○ **Ranager Key Management Service backed by Database**
Ranger Key Management Service backed by Database is a Hadoop Key Management Service implementation that sources encryption zone keys from a backing database and can also store the master key in a backing Hardware Security Module (Luna) for additional security.

○ **A file-based password-protected Java KeyStore**
The file-based Java KeyStore may not be sufficient for large enterprises where a more robust and secure key management solution is required. It is **not suitable** for production use.

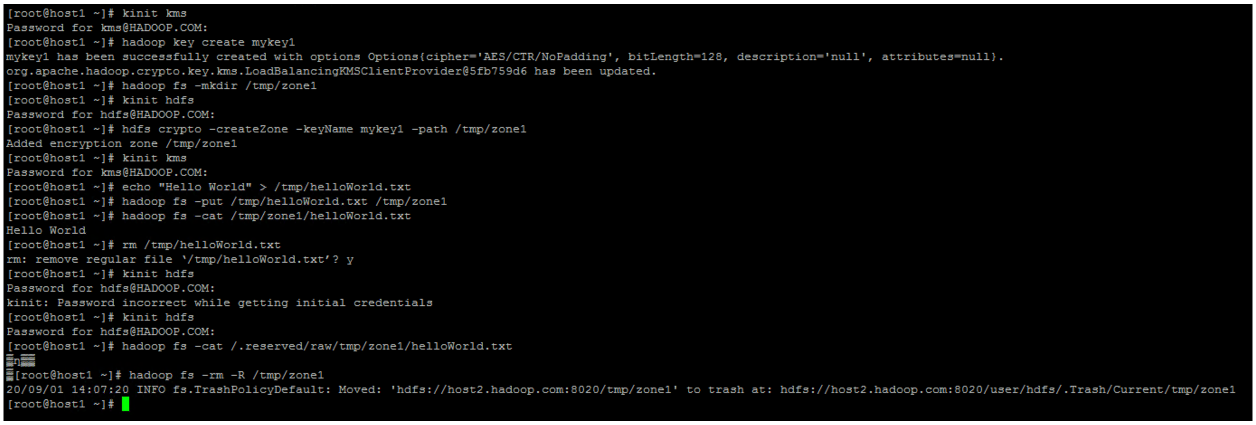
After the root of trust is chosen, a new service called the Hadoop **Key Management Server** (KMS) must be added to your cluster.

The following steps are required to set up HDFS Encryption. Click the links below to complete each step.

Note: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them.

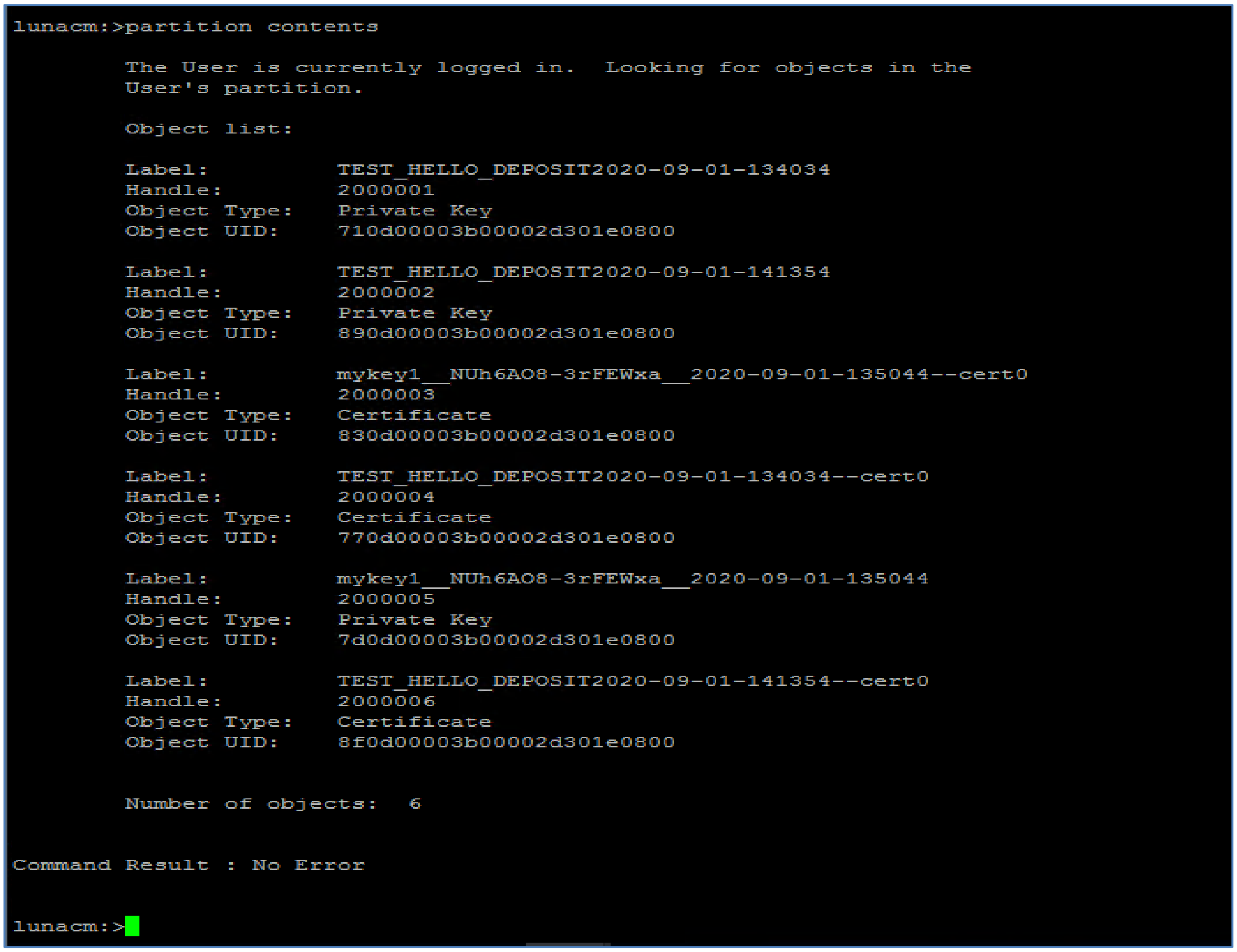
Step		Status	Notes
1	Enable Kerberos	✓ Completed	
2	Enable TLS/SSL	✓ Completed	
3	Add a dedicated cluster for the Key Trustee Servers Add Another	✓ Completed	
4	Install Key Trustee Server binary using packages or parcels	✓ Completed	
5	Add Key Trustee Server Service	✓ Completed	
6	Add Ranger KMS with Key Trustee Server Service	✓ Completed	
7	Restart stale services and redeploy client configuration		
8	Validate Data Encryption		

29. 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
▒n▒▒
▒[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 every time when HSM connectivity with Luna HSM is being checked using curl command or when we run Hadoop command to create the keys.



```
lunacm:>partition contents

        The User is currently logged in.  Looking for objects in the
        User's partition.

        Object list:

        Label:          TEST_HELLO_DEPOSIT2020-09-01-134034
        Handle:         2000001
        Object Type:    Private Key
        Object UID:     710d00003b00002d301e0800

        Label:          TEST_HELLO_DEPOSIT2020-09-01-141354
        Handle:         2000002
        Object Type:    Private Key
        Object UID:     890d00003b00002d301e0800

        Label:          mykey1__NUh6AO8-3rFEWxa__2020-09-01-135044--cert0
        Handle:         2000003
        Object Type:    Certificate
        Object UID:     830d00003b00002d301e0800

        Label:          TEST_HELLO_DEPOSIT2020-09-01-134034--cert0
        Handle:         2000004
        Object Type:    Certificate
        Object UID:     770d00003b00002d301e0800

        Label:          mykey1__NUh6AO8-3rFEWxa__2020-09-01-135044
        Handle:         2000005
        Object Type:    Private Key
        Object UID:     7d0d00003b00002d301e0800

        Label:          TEST_HELLO_DEPOSIT2020-09-01-141354--cert0
        Handle:         2000006
        Object Type:    Certificate
        Object UID:     8f0d00003b00002d301e0800


        Number of objects:  6

Command Result : No Error

lunacm:>
```

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. Refer the Cloudera Documentation for enabling HDFS Transparent Data Encryption.

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.