

Cloudera Data Platform: Integration Guide

THALES LUNA HSM

Document Information

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

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Certified Platforms	4
Certified platforms for Luna HSM	4
Prerequisites	5
Configure Thales Luna HSM	5
Set up Cloudera Data Platform	6
Configuring Ranger KMS using Thales Luna HSM	7
Initializing Ranger KMS with Key Trustee Server to use Thales Luna HSM	16
Contacting Customer Support	29
Customer Support Portal	29
Telephone Support	29
Email Support	29

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 Туре	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- reserved.	-111. Copyright (c) 2020 SafeNet. All rights
Available HSMs:	
Slot Id ->	0
Label ->	Cloudera01
Serial Number ->	1238696044938
Model ->	LunaSA 7.4.0
Firmware Version ->	7.4.0
Configuration -> Cloning Mode	Luna User Partition With SO (PW) Key Export With
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 <u>Luna HSM documentation</u> for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to <u>Luna HSM documentation</u> 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-1.8.0openjdk-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

 Open a web browser and go to <u>http://<server_host>:7180</u>, 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 <u>https://<server_host>:7183</u>, 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**.

C Status - Home - Cloudera Mani × +							– ø ×
← → ♂ ŵ	🛛 🖍 https://host1.hadoop.com:7183	/cmf/home				⊡ ☆	m ⊡ ® ≡
CLOUDERA Manager	Home					Switch to Table View	• • Add •
Search	Status All Health Issues Config	uration 📕 🔹 All Re	cent Corr	nmands			
& Clusters ≅ Hosts	Cluster 1		ı	Charts		30m 1h 2h 6h 12h 1d	7d 30d 🖋 -
🐨 Diagnostics	Cloudera Runtime 7.1.1 (Parcels)				HDFS IO	Cluster Network IO	
Litt. Charts	📀 🗮 4 Hosts				4b/s	997.7K/s 48.8K/s	
Replication Administration	CDP-INFRA-SOLR		1			Press	
	O B HDFS	₽ 6	1		06 AM Total Bytes Read 1b/s = Total Bytes Wr 0.95b/s	06 AM Total Bytes Re 17.9K/s Total Bytes Tr 27.6K/s	
	Ranger		1	Cluster Disk IO	Cluster CPU		
	O 🔮 ZooKeeper	F 1	1	7.6M/s	100%		
	Cloudera Manageme	nt Service		8 5.7M/s 8 3.8M/s 9 1.9M/s	50%		
	Cloudera Manageme	F 4	1	D6 AM	D6 AM		
 ➡ Parcels L§ Running Commands ② Support ③ admin 						Activate Windows Go to Settings to activate W	findows.
«							,

7. Select Ranger KMS and click Continue.

Add Service to Cluster 1 - Clou: × +					- 0
-) → ୯ ଜ	https://host1.hadoop.com:7183/cmf/clust	ters/1546332563/add-service/index	♡ ☆	1	∧ ⊡ ®
C CLOUDERA Manager	🔿 🌞 Key-Value Store Indexer	Key-Value Store Indexer listens for changes in data inside tables contained in HBase and indexes them using Solr.			
	O 🔣 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.			
	O L ^e 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.			
	O Ø Ozone	Apache Hadoop Ozone is a scalable, distributed object store for Hadoop. Not for production use.			
	O đ Phoenix	Apache Phoenix is a scale-out relational database that supports OLTP workloads and provides secondary indexes, materialized views, star schema support, and common Hiller optimizations. Phoenix uses Apache Hillese as the underlying data store.	ie		
	O 1 Ranger	Apache Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform. This service requires Kerberos.			
	Ranger KMS R	Apache Ranger KMS is a Key Management Server. This service is backed by a database for key storage.			
	O Ø 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.			
	O Ø Ranger Raz	Ranger Raz component of Ranger service to enable Ranger authorization to ADLS-Gen2 resources.			
	🔿 📼 \$3 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 B3 filesystem and Hive/Im 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 protocol.	pala the S3A		
🛎 Parcels	🔿 🔹 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 governan introduces operational efficiency by saving and retrieving reusable schema, defining relationships between schemas and enabling data providers and consumers to evolve at d speeds.	ice and ifferent		
C Running Commands	🔿 🥱 Solr	Apache Bolir is a highly scalable, distributed service for indexing and relevance-based exploring of all forms of data.			
0 Support	O 🛃 Spark	Apache Spark is an open source cluster computing system. This service runs Spark as an application on YARN.	Activat	e Windows	
	Can	cel 🗲 Back 🖸	cio to Sett		

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.

C Add Ranger KMS Service to Clu 🗙 🕂						
€ → ୯ û	🔞 🖍 https://host1.hadoop.com:71	83/cmf/clusters/1546332563/add-service/index	?serviceType=RANGER_KMS#step=showDbTes	tConnStep	▽ ☆	li\ ⊡ ©° ≡
CLOUDERA Manager	Add Ranger KMS	Service to Cluster 1				Â
■ Parcels Age Running Commands By Support By Support By Support By Support By Support	Select Dependencies Selec	Setup Database Configure and test database connections. It instalation Guide (2): Ranger KMS Type Postgrad(). • Password • • • • • • • • • • • • •	f using custom databases, create the database Database Hostmame host1.hadoop.com field must match the value you used for the h field must match the value you used for the h atabase is on the same host as the correspon which, it will be used when establishing a corr e services currently support this.	es first according to the Installing and Configu Database Name rangerkma sthame when creating the database. cprin in the Database Notame field, ding role instance. extisn to the database. This customized conr	aring an External Database section of the Successful Username Inngerions Show Password Text Connection wettion URL will override Database Hostname.	

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

G Add Ranger KMS Service to Clu 🗙 🗧					
↔ ⇒ ♂ ŵ	🛛 🕼 https://host1.hadoop.com:71	83/cmf/dusters/1546332563/add-service/index?servic	zeType=RANGER_KMS#step=reviewStep	… ☺ ☆	li\ ⊡ 📽 ≡
CLOUDERA Manager	Add Ranger KMS	Service to Cluster 1			^
	Select Dependencies	Daview Oberges			
	Assign Roles	Review Changes	Danner WHS (Carsion-Mida)	0	
	Setup Database	hadoop.kms.authentication.type	O simple	V	
	(4) Review Changes		erberos erberos		
	5 Command Details	Ranger KMS Load Balancer ranger_kma_load_balancer	Ranger KMS (Service-Wide)	() ()	
	6 Summary	Ranger KMS Master Key Password	Ranger KMS Server Default Group 🕲 Undo	0	
		ranger.db.encrypt.key.password	•••••		
		Enable TLS/SSL for Ranger KMS Server ranger.service.https.attrib.ssl.enabled	Ranger KMS Server Default Group	0	
		Ranger KMS Server TLS/SSL Server JKS Keystore File Location	Ranger KMS Server Default Group	0	
		ranger.service.https.attrib.keystore.file	{(CM_AUTO_TLS})		
		Ranger KMS Server TLS/SSL Server JKS Keystore File Password	Ranger KMS Server Default Group 🐂	0	
		ranger.service.https.attrib.keystore.pass			
		Ranger KMS Server TLS/SSL Client Trust Store File	Ranger KMS Server Default Group •	0	
		xasecure.policymgr.clientssl.truststore			
🚆 Parcels		Password	Kanger KMS Server Default Group		
🖧 Running Commands		xasecure.poincymgr.ciientssi.trustatore.password		_	
 ③ Support ④ admin 				Activate Wind	
«			Back	Continue	ictivate Windows.

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**.

C Add Ranger KMS Service to Clu 🗙			- ø ×
↔ → ♂ ŵ	🛛 🙈 🗝 https://host1.hadoop.com/?183/cmf/dustens/1546332563/add-service/index?serviceType=RANGER_KMS#step=EnishStep	… ⊠ ☆	li\ 🖸 📽 ≡
C CLOUDERA Manager	Add Ranger KMS Service to Cluster 1		î
Parcels A: Ranning Commands Ø Support	 Select Dependencie Araign Roles Setup Database Command Database Command Database Summary 		
🔊 admin 🔣	Back	Go to Sett	

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.

🖸 Status - Home - Cloudera Mani 🗙 🚽	+			- o ×
← → ♂ ☆	🛛 🗟 https://host1.hadoop.com:7183;	/cmf/home		···· 🖂 🏠 🖉 🚍
CLOUDERA Manager	Home			III Switch to Table View 🖉 Add -
Search	Status All Health Issues Config	juration 📕 🗧 🖌 All Re	cent Commands	
& Clusters ≅ Hosts	Cluster 1		Deploy Client Configuration ×	30m 1h 2h 6h 12h 1d 7d 30d ≠+
💖 Diagnostics	Cloudera Runtime 7.1.1 (Parcels)		Are you sure you want to run the Deploy Client Configuration command on cluster Cluster 1?	Cluster Network IO
네. Charts 션) Replication	E 4 Hosts O CDP-INFRA-SOLR		Cancel Deploy Client Configuration	
NA PARTITISTICUT	B HDFS Ranger	ان ک ^و و ان	IS 00.33 = Total Bres Read Ast 5 = Tran Bres Wet 2 Bay I	06.15 06.30 = Total Bytes Re. 20.6K/s = Total Bytes Tr 26.4K/s
	O Ø Ranger KMS	۶ı	I Cluster Disk IO Cluster CPU	
	🗢 🦉 ZooKeeper	F 1	1 0 50%	
	Cloudera Manageme	nt Service		
	Cloudera Manageme			
 Parels /2 Running Commands 9 Support 8 admin 				

- 14. Click Close when successfully deployed all client configurations.
- **15.** On the cluster **Home** page, click the More Options icon (<u>...</u>) and then click **Restart**. Click the **Restart** again when the confirmation window pops up.



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

C Statu	s - Home - Cloudera Mana	< +			-	- 0	×
€ → C	ŵ	🖸 🔒 https://host1.hadoop.com:7183/cmf/home		🖂 🕁	hity	۵ ۵	≡
C CLOU Manag		Home		III Swit	tch to Table View	O Add -	
Search		Status All Health Issues Configuration - All Recent Commands					
🖧 Cluster 🖽 Hosts	Restart				×	d #-	
💖 Diagnor	Status 🛛 🛇 Finished	Context Cluster 1 🗹 🏥 Aug 12, 10:31:33 AM 💿 4.5m					
Littl Charts	All services suc	cessfully restarted.					
C Replica	Show All Steps	Show Only Failed Steps O Show Only Running Steps					
Q. Politini	> 🖉 Execute cor	nmand Stop on cluster Cluster 1	Cluster 1 🕈	Aug 12, 10:31:33 AM	42.58s		
	 Secure con All servit 	nmand Start on cluster 1 ces successfully started.	C Cluster 1 C	Aug 12, 10:32:16 AM	3.8m		
	> 🔿 Execu	te command Start on service Ranger	C Ranger C	Aug 12, 10:32:16 AM	24.14s		
	> 🔿 Execu	te command Start on service ZooKeeper	C ZooKeeper C	Aug 12, 10:32:40 AM	26.17s		
	> 🔿 Execu	te command Start on service Ranger KMS	C* Ranger KMS C*	Aug 12, 10:33:06 AM	29.57s		
	> 🔿 Execu	te command Start on service HDFS	C" HDFS C"	Aug 12, 10:33:36 AM	119.82s		
	Secu	te command Start on service CDP-INFRA-SOLR	CDP-INFRA-SOLR C	Aug 12, 10:35:36 AM	25.52s		
					Close		
Parcels							
Running							
(A) admin							

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

	om:7183/cmf/	services/1546333157/config#		··· 🖂 🕁	III\ E
DERA ger Cluster 1					
Status Instances Cor	MS Ac	clions - Commands Charts Library Audits Quick Lini	a.•		Aug 13, 7:3
Uca Q Search			Filters Role Groups History and Rollback		
ion Filters	NDE:::X 4				
tration SCOPE			ZooKeeper		
Ranger KMS (Service-W Ranger KMS Server	de) 19 114	Ranger KMS Authentication Type	Ranger KMS (Service-Wide)		(?
~ CATEGORY		nadoop.sms.autnentication.type	O simple		
Advanced Database Logs Main Meiniforian	20 6 4 67	Ranger KMS Plugin Hdfs Audit Directory ranger_kms_plugin_hdfs_audit_directory	Ranger KMS (Service-Wide) \$(ranger,base,audit.uri)/kms		C
Performance Ports and Addresses Resource Management Security	1 2 5 6	Ranger KMS Load Balancer ranger_kma_load_balancer	Ranger KMS (Service-Wide)		0
Stacks Collection	5	Ranger KMS Master Key Password ranger.db.encrypt.key.password	Ranger KMS Server Default Group		0
● Error ▲ Warning Edited Non-default	0 0 9	Ranger KMS Max Heapsize ranger_kma_max_heap_size	Ranger KMS Server Default Group		C
Commands	0	Hadoop KMS Blacklist Decrypt EEK hadoop.kms.blacklist.DECRYPT_EEK	Ranger KMS Server Default Group		Aug 13, 72 Nu Nu

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.

Configuration - Ranger KMS - C X	÷					- 0
€ → ୯ û	🛛 🔒 https://host1.hadoop.com:7183/cm	nf/services/1546338618/config#filterfreeText=dbks-site.x	mi		··· 🖂 🕁 📗	n 🗆 📽
C CLOUDERA Manager	Cluster 1					
Search	Status Instances Configuration	Aug 12, 9:33 AM EDT				
E Hosts Cliagnostics Audits	Q dbks-site.xml					
Lat. Charts	Filters				Hide All D	escriptions
 (2) Binglication Administration Administration (2) Administration (3) Funcels (4) Burning Commands (5) Support 	SCOPE Ranger RMS (Envice Wide) Ranger RMS (Envice Wide) CATEGORY Advanced Logis Cope Cope Portamone Portamone Cope Cope	Banger KMS Server Advanced Configuration Snippet (Safety Valve) for confridbks-site.xml	Ranger KMS Server Default Group 🕤 Unde Name Value Description Final	View as XML	For advanced use only. A string to be inserted into conf/dbks-site.aml for this role only.	ø
	Resource Management 0 Becarity 0 Blacks Collection 0 STATUS O Error 0 A Warning 0 Edited 1 Non-default 1 Heas Overrides 0				Per Page 23v	1 - 25 of 132
(A) admin					Go to Settings to activate Win	dows.

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)**.

Configuration - Ranger KMS - 🗆 🗧	+					- 0	×
(← → ଫ ŵ	🛛 🖗 https://host1.hadoop.com	n:7183/cmf/ser	vices/1546333157/config#filterfreeText=HSM		··· 🗵 🏠	lii\ 🖸 🏽	8 ≡
C CLOUDERA Manager	Security Stacks Collection	0	Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/dbks-site.xml	Ranger KMS Ser	ver Default Group 💊 View	⑦ v as XML	^
Search	V STATUS			Name	ranger.ks.hsm.enabled	⋳⊕	
& Clusters	© Error A Warning	0		Weber			
I Hosts	Edited	0		Value	rue		
👽 Diagnostics	Has Overrides	0		Description	Enable HSM Encryption		
Audits							
					Final		
				Nama	ranger is here tune		
Administration				1441110	ranger-no-memorype	500	
				Value	LunaProvider		
				Description	Luna HSM Type		
					Final		
				Name	ranger.ks.hsm.partition.name	⋳⊕	
				Value	ClouderaHA		
				Description	Luna HSM Partition Name		
					Final		
				Name	ranger.ks.hsjn.partition.password] 🕀 🌐	
- Darasla							
Running Commands				Value	userpin i		
Support				Description	Luna HSM Partition Password		
(A) admin					Activate Window Go to Settings to activ		
«					Sa	ve 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.

s - Ranger KMS - Cloudera X	× +					- 6
C 6	https://host1.hadoop.com:7183/cmf/services/1546333157/status				🖂 🕁	lii\ 🖸
CLOUDERA Manager	Cluster 1					
rch	🗢 🗑 Ranger KMS 🛛 🗚 🕁				4 30 minutes preceding Aug	3, 7:49 AM EDT 🕨 🕅
lusters	Status Instances Configuration Restart needed	Audits Quick Links 👻				
	Health Tests	Create Trigger	Charte		30m 1h 2h 6i	12h 1d 7d 30d 🖋
	Health Tests		Charts			
	Ranger KMS Server Health Healthy RANGER, KMS, SERVER: 1. Concerning RANGER, KMS, SERVER: 0. RANGER, KMS, SERVER: 1. Percent healthy: 100.00%. Percent healthy or con- tended to the server of the s	Suppress Total ncerning: 100.00%.	Important Events and Alerts @	Informational Events ©		
	Status Summary		07:30 07:45	07:30	07:45	
	Ranger KMS Server O 1 Good Health		Alerts 0 Critical Events 0 = Important Events	Ranger KMS, Informational Events 0		
	Hosts O 1 Good Health					
	Health History Range KMS Server Health Good > I Became Good	7:01:46 AM 🚦				
	Ranger KMS Server Health Bad 1 Became Bad	7:01:31 AM 🚦				
	 Ranger KMS Server Health Good > 1 Became Good 	6:45:01 AM 🚦				
	Ranger KMS Server Health Disabled Became Disabled	6:27:21 AM 🚦				
dmin						

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.

Stale Configurations - Clouden × +					- ø ×
(←) → ♂ ŵ	0 🔒 https://host1.hadoop.com	m :7183/cmf/d	iters/1546332563/staleness/view?service=ranger_kms	🖂 🏠	III\ 🗊 🐨 🗏
CLOUDERA Manager	Cluster 1				÷
Search	Stale Configura	tions			
Costars El Horsts © Diagnostics A Audits Lat Charts (2) Replication © Administration	Filters ← FILE File: cont/dblasstassmit ← SERVICE ← Ranger KMS Server Ranger KMS Server	Clear All I Clear I I I I I I I I I I I I I I I I I I I	File: conf/dBs-site.unl		ranger_kas(1) Shoe
 Parcela & Running Commanda Support admin 				Activate W Go to Settings	findows La activate Windows Restart Stale Services

Back Restart Now

- Cloudera Manager € → ୯ û ... ⊡ ☆ lii\ 🗉 📽 ≡ £ C CLOUDERA Manager Restart Stale Services 1 Review Changes **Review Changes** 2 Command Details All services running with outdated configuration ons in the cluster and their dependencies will be restarted Re-deploy client configuration # Parcel
- 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.

C Status - Ranger KMS - Cloudera X	+					– ø ×
← → ♂ ☆	🛛 🚯 https://host1.hadoop.com:7183/cmf/services/1546333157/sta	tus			… ☺ ☆	li\ ⊡ ©° ≡
CLOUDERA Manager	Cluster 1					^
Search	🛇 🗑 Ranger KMS 🛛 Actions 🗸			**	30 minutes preceding Aug 13, 9:43	BAMEDT 🕪 🕪 🖿
BE Hosts	Status Instances Configuration Commands Charts Lib	rary Audits Quick Links 🕶				
🍄 Diagnostics	Health Tests	Create Trigger	Charts		30m 1h 2h 6h 12h	1d 7d 30d 🖋 🗸
네 Charts 션] Replication ✿ Administration	Ranger KMS Server Health Healthy RANGER_VMS_SERVER: 1. Concerning RANGER_VMS_SERV RANGER_VMS_SERVER: 1. Percent healthy: 100.00%. Percent healthy	Suppress YER: 0. Total y or concerning: 100.00%.	Important Events and Alerts ©	Informational Events @		
	Status Summary		09:15 09:30	09:15 09:30		
	Ranger KMS Server 📀 1 Good Health		Alerts 0 — Critical Events 0 — Important Events 0	 Ranger KMS, Informational Events 0 		
	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 🚦				
🚔 Parcels 😅 Running Commands	Ranger KMS Server Health Disabled 1 Recame Disabled	9:35:14 AM 🚦				
A admin					Activate Window: Go to Settings to active	S ste Windows.

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 :7180">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 <u>https://<server_host>:7183</u>, 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
00:00:00
```

| 2.9 kB

```
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
                 16 M
  cloudera-repol
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
         00:00:00
  | 16 MB
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

- After the setup is completed, the Key HSM configuration is stored in /usr/share/keytrustee-serverkeyhsm/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+zO1chr90Kbb4qr17
jWHYje+vfxsPT8cQ5w36iqRJBZq7nIQ4dY/qireBMzdrO1mCS8e9qsg8u5qmejkOv00oesHRoXS
bNbBHnaDb044SxtKRyhNrKVPYU5Hk4c18Q/4zfvIZiXGIWM6SdKGq/U144E6BQoS/5/t5PhIn5Y
J3yoi5RK4U3ah2pJJOiz/mQBxHK8L1xnv74DO+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
```

 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 --clientcertfile and --client-keyfile options to specify the path to default certificate and key.

```
# ktadmin keyhsm --server <u>https://127.0.0.1:9090</u> --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, $% \left({{{\left({{{\left({{{\left({{{c}} \right)}} \right.}} \right)}_{0}}}} \right)$

items stored in the HSM must remain there!

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

Migrating hsm deposits...

Migration Complete!

- -----
- 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 <u>https://host5.hadoop.com:11371/test hsm</u>

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.

- 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.

C Add Ranger KMS with Key Trust × +					- ø ×			
← → C ^e û	n:7183/cmf/clusters/1546332563/add	service/index?serviceType=RANGER_	KMS_KTS#step=initialAjaxStep0	··· 🖂 🕁	⊻ ⊪\ ⊡ ®' :			
C CLOUDERA Add Ranger KM	Add Ranger KMS with Key Trustee Server Service to Cluster 1							
C CCOUSERA Add Ranger KM C Conversion C Select Dependencies C Se	S with Key Trustee : Getting Started Hadoop interacts with the Key Choose Key Trustee Server	Server Service to C Management Server (KMS) to store © Existing Key Trustee Server hoetS.hadoop.com © External Key Trustee Server Active Key Trustee Server	luster 1 and retrieve encryption keys. Peasive Key Trustee Server Peasive Key Trustee Server					
Support admin				Activa	te Windows			
«				Go to Se Back Continue	ttings to activate Windows.			

- 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**.

C Add Ranger KMS with Key Trust 🗶 🚽	+		- 0
← → ♂ ŵ	🛿 🐁 https://host1. hadoop.com:7183/cm//dusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=ajarStep1	☺ ☆	± m⁄ ⊡ ®
CLOUDERA Manager	Add Ranger KMS with Key Trustee Server Service to Cluster 1		
	Certing Started Certing Started Select Dependencies Casign Roles Certify Select Dependencies Certify Select Depen	on is required to register with Key	
	 (i) Setup Authorization Servet (ii) Setup TLS for Ranger KMS with Key Truste Server (iii) Review Changes (iiii) Command Details (iii) Superiodincy (iiii) Superiodincy (iii) Summary 		
 # Parcels # Running Commands Bupport @ admin 		Activate V Goussener	Vindows s to activate Windows.

- 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.

C Add Ranger KMS with Key Trust ×					- ø ×
€ → ሮ û	🔞 https://host1.hadoop.com:718	33/cmf/dusters/1546332563/add-service/index?serviceType=RANGER_KMS_KTS#step=commandDetailsStep		ເ ☆	⊻ ⊪\ ⊡ 📽 🖻
C CLOUDERA Manager	Add Ranger KMS v	with Key Trustee Server Service to Cluster 1			
Getting Started Gelect Dependencies Assign Roles Setup Entropy		First Run Command Status • Finished Context Ranger KMS with Key Trustee Server (2) Entished First Run of the following services successfully: Ranger KMS with Key Trustee Server. • <u>completed 1 of 1 step().</u> • Show All Steps O show Only Failed Steps			
	Setup Authorization Secret	☑ ● 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	
	with Key Trustee Server	> Execute 2 steps in sequence	Sep 1, 8:23:09 AM	5.24s	
♣ Parcels	Review Changes Command Details Synchronize Private Keys and HDPS Dependency Sammary				
 Ø Support A admin 				Activa	
«			Back	Continue	rungs to activate windows.

C Add Ranger KMS with Key Trust 🗙	+				- 1	ø	×
← → ⊂ ŵ	🛛 🔒 https://host1.hadoop.com:718	3/cmf/dusters/1546332563/add-service/index?serviceFiype=RANGER_KMS_KTS#step=finishStep **	· 🖂 🕁	ł	2 111 12	1	- <u>@</u>
CLOUDERA Manager	Add Ranger KMS v	with Key Trustee Server Service to Cluster 1					^
	 Detting Started Belect Dependencies Assign Roles Betap Entropy Betap	Summary Not new Key Trustee KMS service is installed and configured on your cluster.					
Parcels							
🖧 Running Commands							
Support A admin			Activate				
«		Back	Go to Sett Finish	ings to activate	Window	5.	

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.

Status - Home - Cloudera Mani X	t				- 6 - 3
€ → ሮ û	🛛 🔒 https://host1.hadoop.com:7183/cmf/home				···⊡☆ ¥ II/ □ @
CLOUDERA Manager	Home				III Switch to Table View Add -
Search	Status All Health Issues Configuration 🗲 11 - All	Recent Com	mands		
	Cluster 1	÷	Charts		30m 1h 2h 6h 12h 1d 7d 30d 🖋 -
Audits	Cloudera Runtime 7.1.1 (Parcels)			HDFS IO	Cluster Network IO
Latt Charts 伦 Replication 후 Administration	O ■4 Hosts			927/2/4 48.8X/9 08.AM 08.15	
	C S HDFS ✓ 6 U B	1			08 AM 08:15 Oluster 1, Total. 150K/s =Cluster 1, Total. 175K/s
	Stale Configuration: Res needed	start	Cluster Disk ID	Total Bytes Rea 1.2K/s Total Bytes Wri 109K/s	Cluster 2, Total 475b/s =Cluster 2, Total 193b/s
	O 🔞 Ranger KMS with Ke 📕 1	1		Cluster CPU	
	🗢 🖤 ZooKeeper 🛛 🗲 1	1		50%	
	Cluster 2	ł.	00 AM 00:15 = Chaster 1, Total3.5K/s = Chaster 1, Total3.3K/s	06 AM 00:15	
	Cloudera Runtime 7.1.1 (Parcels)				
	E 1 Hosts				
	Key Trustee Server	1			
	Cloudera Management Service				
	Cloudera Manageme	1			
Parcels Support Support Annin					Activate Windows Go to Settings to activate Windows.

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

Cloudera Manager X	(+					-	- 6
-)→ ୯ û	M https://host1.hadoop.com A	n:7183/cmf/clusters/1546332563/staleness/restartWizard?returnUrl=%2Fcmf%2Fhome#step=commandDetai	isStep		··· 🖂 🕁	⊥ ⊥	
CLOUDERA Manager	Restart Stale Se	rvices					
	 Review Changes Command Details 	Restart Awaiting Staleness Computation Command Sutu @ Finished Context Cluster1 (2)					
	 Execute global command Wait for configuration staleness computation Configuration staleness computation completed. 	C.	Sep 1, 8:35:04 AM	221ms			
	 Execute command Restart on cluster Cluster 1 All services successfully restarted. 	Cluster 1 C	Sep 1, 8:35:05 AM	3.5m			
		> S Execute command Stop on cluster Cluster 1	Cluster 1 C	Sep 1, 8:35:05 AM	42.41s		
		 Execute command Start on cluster Cluster 1 All services successfully started. 	Cluster 1 C	Sep 1, 8:35:47 AM	2.4m		
		> Execute command Start on service Ranger	C* Ranger C*	Sep 1, 8:35:48 AM	26.27s		
		> Execute command Start on service HDFS	C HDFS C	Sep 1, 8:36:14 AM	95.01s		
		> C 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 1 Successfully deployed all client configurations.	Cluster 1 C	Sep 1, 8:38:14 AM	18.45s		
		Secure DeployClusterClientConfig for (solr,hdfs) in parallel.		Sep 1, 8:38:14 AM	18.44s		

- 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.

G Status - Home - Cloudera Mari X	F							- 0	×
€ → ୯ û	🛛 🗟 https://host1.hadoop.com:7183	l/anf/home				··· 🖂 🕁	₹ III/	•	II,
CLOUDERA Manager	Home					100 Sv	ritch to Table View	O Add +] ^
Search	Status All Health Issues Confi	guration 🛃 👻 All Recer	nt Commi	ands					
🚯 Clusters									
Hosts	Cluster 1		1	Charts		30m	ih 2h 6h 12h 1d 7d	30d 🧨 -	
♥ Diagnostics	Cloudera Runtime 7.1.1 (Parcels)				HDFS IO	Cluster Network IO			
Lal. Charts	🔿 🗮 4 Hosts	\$ 2			977K/a	8 977K/s			
(신) Replication	COP-INFRA-SOLR		1		a 488K/s	phies	~~		
 Administration 	O B HDFS	F 6	1		05.45 05 AM — Total Bytes Res 577b/s — Total Bytes Wit 107K/s	Cluster 1, Totel 148K/s Cluster 1	Total 159K/s		
	O Ranger		1			Cluster 2, Total 6698/s =Cluster 2	lotal _ 773b/s		
	Ranger KMS with Ke		1	Cluster Disk IO	Cluster CPU				
	ZooKeeper	11	1	977R/1	50% d				
	Cluster 2			08.45 09.AM = Chuster 1, Tota 20.35% = Chuster 1, Total 561W/s - Chuster 3, Total	08.45 09.4M				
	Cloudera Runtime 7.1.1 (Parcels)				- CONTR 1 4.6% - CONTR 2 4.5%				
	💿 🧮 1 Hosts								
	Key Trustee Server		1						
	Cloudera Manageme	ent Service							
	😒 🧿 Cloudera Manageme		1						
Parcels Running Commands									
② Support ③ admin							Windows ngs to activate Wind		
🛯 🔎 🗩 🖉	👏 🖻						ا ی م	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.

	https://host1.hadoop.com/7183/cmt/clusters/1546332563/hdfsEncryption	··· 🗵 🕁	± ш/		
CLOUDERA Manager	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 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 (2).	, data can be encrypted and			
	The root of trust for encryption keys can either be: Branger 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.
	O 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 (up. and a source) and a security.			
	O 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 (0MS) must be added to your cluster.				
	The following steps are required to set up HDFS Encryption. Click the links below to complete each step.				
	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	Notes			
	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 1 Enable Karberos	Notes			
	The following steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. 3tep Status 1 Enable Karberos Image: Completed	Notes			
	The following steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. Step Status 1 Enable Keberos	Notes			
	The following steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. Step Status 1 Enable Kerberos Completed 2 Enable TLS/SSL Completed 3 Add a dedicated cluster for the Key Trustee Servers Add Another Completed 4 Instal Key Trustee Servers Add Another Completed	Notes			
	Image: Steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. Step: Status 1 Enable Karberos Completed 2 Enable TLS/SSL Completed 3 Add a dedicate cluster for the Key Trustee Servers Add Another Completed 4 Install Key Trustee Server Service Completed 5 Add Key Trustee Server Service Completed	Notes			
	Image: Steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. Step Status 1 Enable Karberos Completed 2 Enable Karberos Completed 3 Add a dedicated cluster for the Key Trustee Servers Add Another Completed 4 Install Key Trustee Server Service Completed 5 Add Key Trustee Server Service Completed 6 Add Runger KMS with Key Trustee Server Service Completed	Notes			
	Image: Steps are required to set up HDFS Encryption. Click the links below to complete each step. Nete: This workflow will not encrypt data automatically. You must manually create encryption keys and encryption zones and move data into them. Step Status 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 Service Completed 5 Add Key Trustee Server Service Completed 6 Add Runger KMS with Key Trustee Server Service Completed 7 Restart state services and redeploy Client configuration Completed	Notes			

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.
<pre>[root@host1 ~]# hadoop fs -mkdir /tmp/zone1</pre>
[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 ~]
≣[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.

lunacm:>partition contents					
	The User is currently logged in. Looking for objects in the User's partition.				
	Object list:				
	Label: Handle:	TEST_HELLO_DEPOSIT2020-09-01-134034 2000001			
	Object UID:	710d00003b00002d301e0800			
	Label: Handle:	TEST_HELLO_DEPOSIT2020-09-01-141354 2000002			
	Object Type:	Private Key			
	Object Oib:	890000030000230120800			
	Label: Handle:	mykey1NUh6A08-3rFEWxa2020-09-01-135044cert0 2000003			
	Object Type:	Certificate			
	Object UID:	830d00003b00002d301e0800			
	Label:	TEST_HELLO_DEPOSIT2020-09-01-134034cert0			
	Handle:				
	Object UID:	770d00003b00002d301e0800			
	Label:	mykey1 NUh6A08-3rFEWxa 2020-09-01-135044			
	Handle:	2000005			
	Object Type:	Private Key			
	Object UID:	7404000036000024301e0800			
	Label:	TEST_HELLO_DEPOSIT2020-09-01-141354cert0			
	Handle:	2000006			
	Object UID:	Sf0d00003b00002d301e0800			
	Number of objects: 6				
Command	Command Decult , No Exper				
Command Result : NO EFFOR					
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.

Contacting Customer Support

If you encounter a problem at any stage during this integration, contact <u>Thales Customer Support</u>. 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 <u>https://supportportal.thalesgroup.com</u>, 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.