THALES

Hortonworks Data Platform: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-000380-001
Revision	B
Release Date	5 January 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

This guide demonstrates setting up a Ranger KMS component inside Hortonworks Data Platform (HDP) and configuring the Ranger KMS to use Luna HSM devices or Luna Cloud HSM services for securing the master key for HDP operations. HDP includes a data storage environment called the Hadoop Distributed File System (HDFS). HDFS data at rest encryption implements end-to-end encryption of data read from and written to HDFS. HDFS data at rest encryption encrypts selected files and directories stored ("at rest") in HDFS. This approach uses specially designated HDFS directories known as "encryption zones." Apache Ambari, part of HDP, allows enterprises to plan, install, and securely configure HDP, thus making it easier to provide ongoing cluster maintenance and management. HDP uses Apache Ranger to provide centralized security administration and management. Apache Ranger uses the Ranger Key Management Service (KMS), an open source and scalable cryptographic key management service supporting HDFS "data at rest" encryption.

The benefits of integrating Luna HSM and Luna Cloud HSM with Hortonworks Data Platform include:

- Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of keys.
- HSM audit trail*.
- Significant performance improvements by off-loading cryptographic operations from application servers.

*Luna Cloud HSM service does not have access to the secure audit trail

Certified Platforms

This integration is certified on the following platforms:

HSM Type	Platforms Certified
Luna HSM	RHEL 7

NOTE: This integration is tested in both HA and FIPS mode. However, Luna HSM firmware v7.7.0 does not supports the FIPS mode.

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. The 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.

HSM Type	Platforms Certified
Luna Cloud HSM	RHEL 7

Luna Cloud HSM: Luna Cloud HSM platform provides on-demand, cloud-based HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

Configuring Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the Luna HSM documentation for more information.
2. Create a partition that will be later used by Hortonworks.
3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the 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) v10.3.0-275. Copyright (c) 2020 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->              0

Label ->                HortonWorks

Serial Number ->        1238696044952

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
```

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

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

Controlling User Access to HSM

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.

To add a user to hsmusers group

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. You must log in again to see the change.

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

Set up Luna HSM High-Availability

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

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   ```

```
[Linux]
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
[Linux]
Source the setenv script.
# source ./setenv
```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   Cloud HSM Certificates:

```
server-certificate.pem
partition-ca-certificate.pem
partition-certificate.pem
```

   LunaClient Certificate Directory:

```
[Windows default location for Luna Client]
C:\Program Files\Safenet\Lunaclient\cert\
[Linux default location for Luna Client]
/usr/safenet/lunaclient/cert/
```

   NOTE: Skip this step for Luna Client v10.2 or higher.

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

```
[Windows]
crystoki.ini
[Linux]
Chrystoki.conf
```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

```
[XTC]
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
```

```
. . .

[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

NOTE: Skip this step for Luna Client v10.2 or higher.

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>

[Windows Default]

C:\Program Files\Safenet\Lunaclient\plugins\

[Linux Default]

/usr/safenet/lunaclient/plugins/
```

Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

Windows

In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

Linux

Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

11. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

NOTE: Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up Hortonworks Data Platform

You need to set up and configure the Hortonworks Data Platform (HDP) for integration with the Luna HSM or Luan Cloud HSM service. This will involve installing HDP and Apache Ambari on the system and then using Apache Ambari to install HDFS and Ranger KMS.

1. Set the **hostname** of the client machine to be `master.hadoop.com`

   ```
   # hostnamectl set-hostname master.hadoop.com
   ```

2. Install Hortonworks Data Platform (HDP). For detailed instructions, follow the HDP Command Line Installation documentation.
3. Install Apache Ambari. For detailed instructions, refer to Apache Ambari Installation.
4. Ranger KMS requires HDFS and Ranger. Use Apache Ambari to install HDFS and Ranger on the system. Refer to the HDFS "Data at Rest" Encryption and the Ranger Using Ambari documentation for detailed installation procedures.
5. Add the following setting to `./bash_profile` of **kms** user when using Luna Cloud HSM service:

   ```
   export ChrystokiConfigurationPath=<DPOD client directory>
   ```

Integrating Hortonworks Data Platform with Luna HSM

Integrate Luna HSM or HSM on Luna Cloud HSM service with the Ranger Key management Service to secure the encryption keys for Hortonworks Data Platform within the HSM.

Configure java.security file

Configure the Luna HSM or Luna Cloud HSM service java.security file to use the Luna Provider. To configure the java.security file:

1. Edit the Java Security Configuration file java.security located in the directory <JDK_installation_directory>/jre/lib/security

   Add the Luna Provider section to the java.security file, as shown below:

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

2. Make secret keys extractable. Add the following piece of code to the java.security file:

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

   Save the changes to the java.security file.

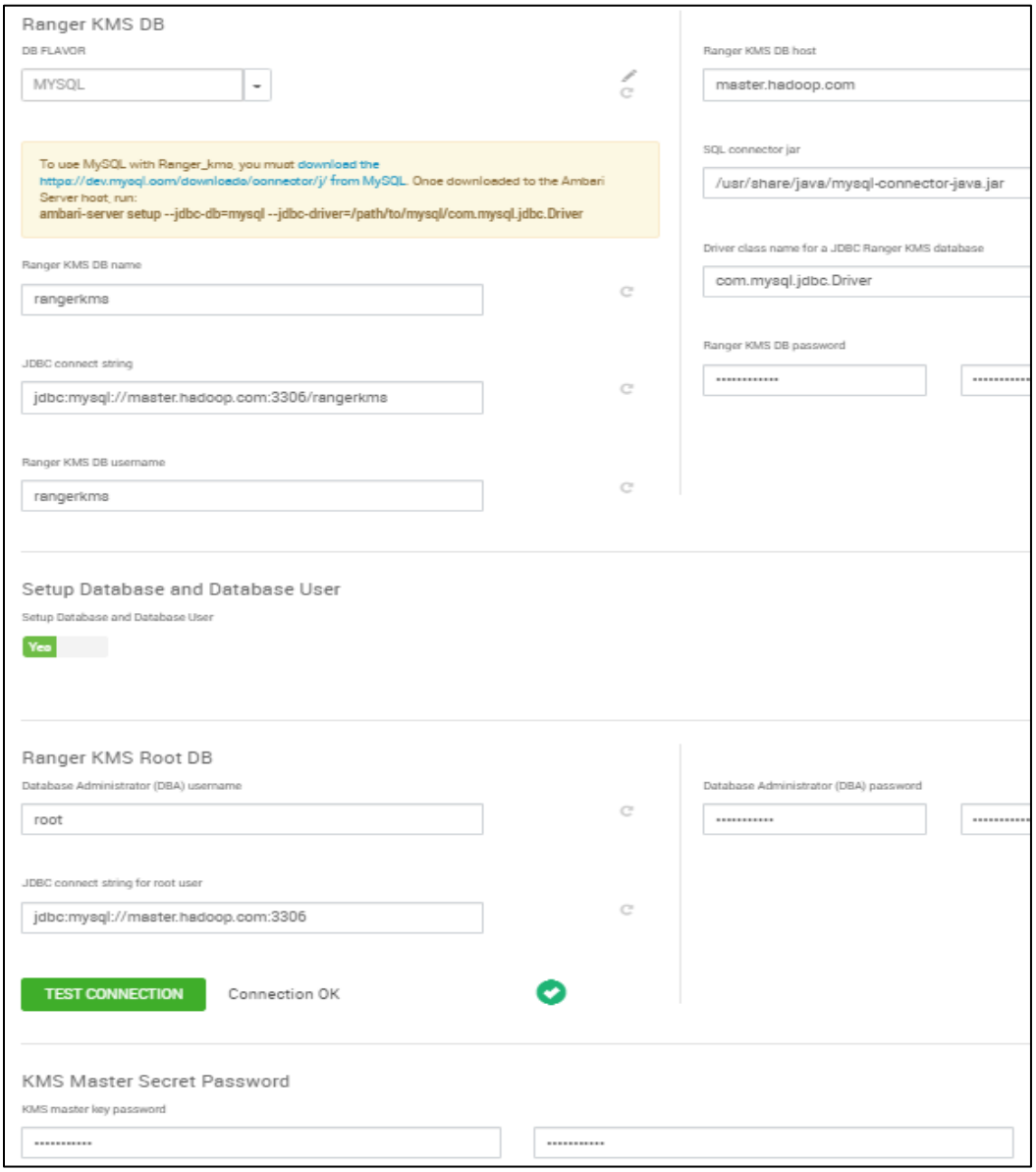
3. Copy the libLunaAPI.so and LunaProvider.jar from the `<Luna_installation_directory>/jsp/lib` folder to the Java extension folder under `<JDK_installation_directory>/jre/lib/ext`.

Setting up Ranger KMS

Follow these steps to configure Ranger KMS to use the Luna Network HSM or Luna Cloud HSM service for generating and storing the applications master key:

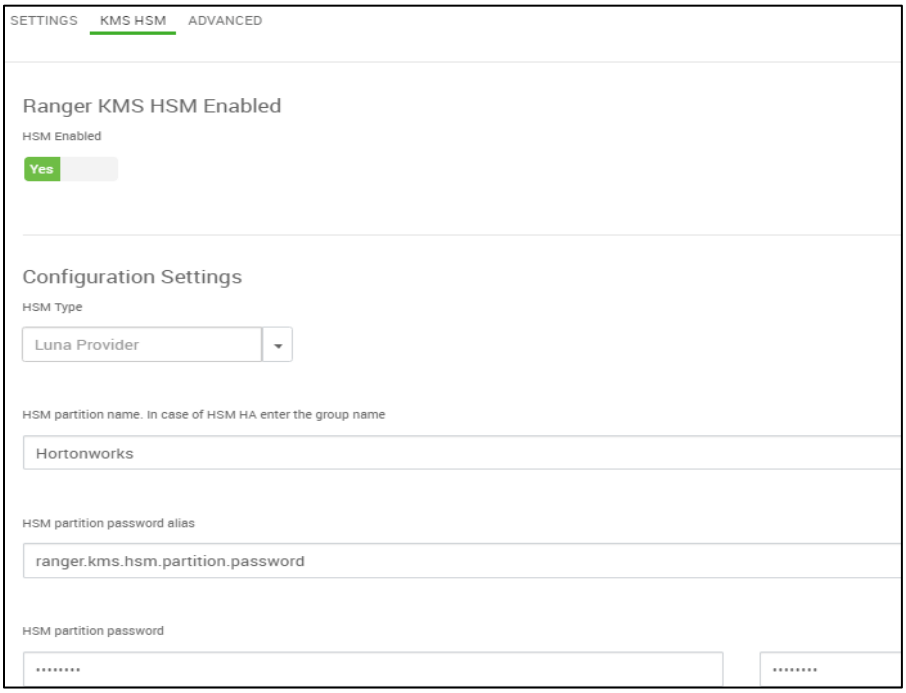
1. Log in as admin to Ambari Web UI on http://<IP-Address>:8080.
2. Go to **Services** and click **Add Service**. An **Add Service** wizard will appear on the screen.
3. Select **Ranger KMS** from the **Choose Services** list. Click **Next**.
4. Under **Assign Masters**, choose the host you want the Ranger KMS to run on and click **Next**.
5. Under **Customize Services**, set the required values (marked in red).
6. Set the **Ranger KMS DB FLAVOR** to MYSQL.
7. Under **Ranger KMS DB Host,** specify the hostname of the machine (for example `master.hadoop.com`).
8. Under **SQL connector jar,** specify the location of `mysql-connector-java.jar`.
9. Enter the **Ranger KMS DB name**, **Ranger KMS DB username** and **Ranger KMS DB password**.
10. Toggle **Setup Database and Database User** to **Yes**.
11. Under **Ranger KMS Root DB** section, specify the root password of the database in the **Database Administrator (DBA) password** field.
12. Click **Test Connection**. It should report **Connection OK**.

13. Enter and confirm the **KMS master key password**.



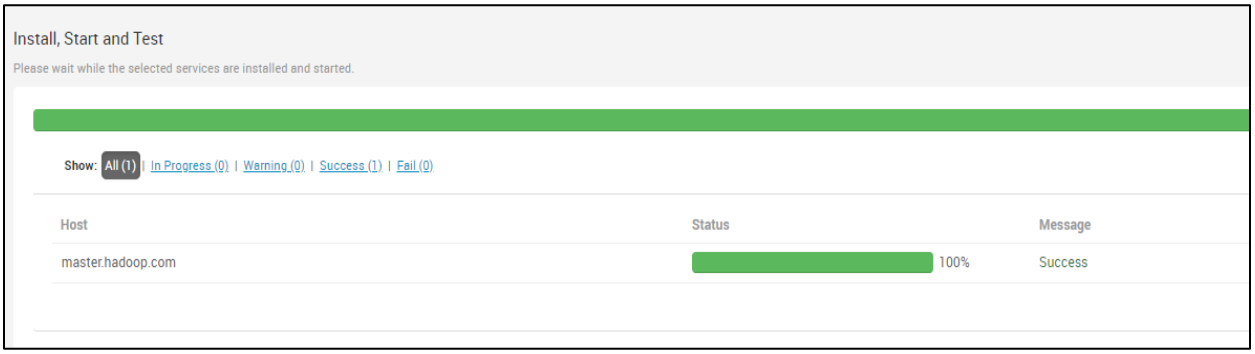
14. Under **KMS-HSM** section, toggle **HSM Enabled** to **Yes**.
15. Under **Configuration Settings**, specify Luna HSM or Luna Cloud HSM service details.
16. Open the **HSM Type** drop-down menu and select **Luna Provider.**
17. Enter the **HSM partition name**.

18. Enter the **HSM partition password**.



19. Click **Next**.

20. In the **Review** pane, verify all the settings and click **Deploy**. Monitor the progress of installing, starting, and testing the service. When the service installs and starts successfully, click **Next**.



The **Summary** screen displays the results. Choose **Complete**.

21. Restart the **HDFS**, **Ranger** and **Ranger KMS** services. The master key generates on the HSM partition. Verify the key exists by executing **partition contents** in lunacm:

```
[root@master 64]# ./lunacm
LunaCM v1.1.0-1044. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              3
        Label ->                Hortonworks
        Serial Number ->        1312452125648
        Model ->                Cryptovisor7
        Firmware Version ->     7.1.3
        CV Firmware Version ->  1.1.0
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     User Token Slot


        Current Slot Id: 3

lunacm:>role login -n co

        enter password: ********

Command Result : No Error

lunacm:>partition contents

        The 'Crypto Officer' is currently logged in.  Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:         RangerKMSKey
        Handle:        2144185232
        Object Type:   Symmetric Key
        Object UID:    0543000013000001ee990800


        Number of objects:  1


Command Result : No Error
```

This completes the integration of Hortonworks Data Platform with Luna HSM or Luna Cloud HSM service.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or 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.