

Ranger KMS Luna HSM Support

- [Link for SafeNet Luna SA Client Installation:](#)
- [Installing Ranger KMS HSM \(Manually\)](#)
- [Installing Ranger KMS HSM \(Ambari\)](#)
- [Configure HSM HA](#)
- [Installation of Ranger KMS HSM HA](#)
- [Migration](#)
 - [HSM to Ranger DB](#)
 - [Ranger DB to HSM](#)
- [Clear Objects from HSM partition](#)

Note: Below steps are useful for Ranger installed with version 0.5.0 using Ambari



For any setup/execution of Ranger KMS related to HSM please check "java.security" file for inclusion of "LunaProvider" in provider list as well as property "createExtractableKeys" to true for Luna AS MENTIONED IN STEP 1.12. Also we need a separate partition for each KMS cluster

- **Link for SafeNet Luna SA Client Installation:**

http://cloudhsm-safenet-docs.s3.amazonaws.com/007-011136-002_lunasa_5-1_webhelp_rev-a/Content/configuration/configuration_setup_luna_sa_after_installation.htm

- **Installing Ranger KMS HSM (Manually)**

1. Extract the Ranger KMS tar
2. Install Ranger-kms with appropriate property values
 - a. Go to ranger-kms folder and edit install.properties (Enter appropriate values for the below given properties)

```
db_root_user=  
db_root_password=  
db_host=  
db_name=  
db_user=  
db_password=  
HSM_TYPE=LunaProvider  
HSM_ENABLED=  
HSM_PARTITION_NAME=  
HSM_PARTITION_PASSWORD=  
KMS_MASTER_KEY_PASSWORD=  
POLICY_MGR_URL=  
REPOSITORY_NAME=  
XAAUDIT.DB.IS_ENABLED=  
XAAUDIT.DB.FLAVOUR=  
XAAUDIT.DB.HOSTNAME=  
XAAUDIT.DB.DATABASE_NAME=  
XAAUDIT.DB.USER_NAME=  
XAAUDIT.DB.PASSWORD=
```

3. Edit "hdfs-site.xml"

- a. Perform following steps:
 - i. Go to path : /usr/hdp/<version>/hadoop/conf/
 - ii. vim hdfs-site.xml
 - iii. For property "dfs.encryption.key.provider.uri", enter the value "kms://http@<ranger_kms host name>:9292/kms"
 - iv. save and quit

4. Edit "core-site.xml":

- a. Perform following steps:
 - i. Go to path: /usr/hdp/<version>/hadoop/conf/
 - ii. vim core-site.xml
 - iii. For property "hadoop.security.key.provider.path", enter the value "kms://http@<ranger_kms host name>:9292/kms"
 - iv. save and quit

5. Restart Namenode :

```
su --l hdfs --c "/usr/hdp/<version>/hadoop/sbin/hadoop-daemon.sh stop namenode"
su --l hdfs --c "/usr/hdp/<version>/hadoop/sbin/hadoop-daemon.sh start namenode"
```

6. Run the setup by command : ./setup.sh

7. Start the KMS server by command: ranger-kms start

• Installing Ranger KMS HSM (Ambari)

Two Approach are possible

Approach 1 :(Configuring with plain text password)

1. Add Ranger KMS Service
2. While configuring add the HSM related properties in "custom dbks-site" accordon.
 - a. ranger.ks.hsm.enabled=true
 - b. ranger.ks.hsm.partition.name=<Partition Name>
 - c. ranger.ks.hsm.partition.password=<Partition Password>
 - d. ranger.ks.hsm.type=LunaProvider

[blocked URL](#)

3. Click on Next and follow the instructions to install Ranger KMS.

Approach 2 : (Configuring without plain text password and using jceks)

1. Add Ranger KMS Service
2. While configuring add the HSM related properties in "custom dbks-site" accordon.
 - a. ranger.ks.hsm.enabled=true
 - b. ranger.ks.hsm.partition.name=<Partition Name>
 - c. ranger.ks.hsm.partition.password=_
 - d. ranger.ks.hsm.partition.password.alias=ranger.kms.hsm.partition.password
 - e. ranger.ks.hsm.type=LunaProvider

[blocked URL](#)

3. Click on Next and follow the instructions to install Ranger KMS. (Note Ranger KMS will not start it will fail to start)
4. Execute below command on cluster where Ranger KMS is installed.

```
python /usr/hdp/current/ranger-kms/ranger_credential_helper.py -l "/usr/hdp/current/ranger-kms/cred
/lib/*" -f /etc/ranger/kms/rangerkms.jceks -k ranger.kms.hsm.partition.password -v
<Partition_Password> -c 1
```

5. Restart the KMS from Ambari

• Configure HSM HA



For this section you need at least two Luna SA appliances with PED Authentication, or two with Password Authentication.

1. Set up Appliances for HA

- a. Perform the network setup on your two HA units as mentioned in step 1(Client software installation)
- b. Ensure that the Allow Cloning and Allow Network Replication policies are "On" in hsm showPolicies
- c. Initialize the HSMs on your Luna SA appliances. They must have the same cloning domain – that is, they must share the same red, domain PED Key if they are PED-authenticated , or they must share the same domain string if they are password-authenticated.
- d. Create a partition on each Luna SA. They need not have the same labels, but must have the same password.
- e. Make a note of the serial number of each Partition created on each Luna SA (use partition show).

2. Register Clients with Luna SA HA

- a. Proceed with normal client setup as mentioned in step 2.(Create a Network Trust Link between the Client and the Appliance).
- b. Register your client computer with both Luna SAs
- c. Verify using **.jvtl** verify command. It should show the no's of partition registered with client

3. Create the HA Group

Note: Please follow the appropriate steps to form HSM HA according to your client version.

a. **Version 6**

Client software for HSM **Version 6** :

- i. After creating partitions on (at least) two Luna appliances, and setting up NTLS between those partitions and your client, use LunaCM to configure HA on your client
 1. Go to directory: /usr/safenet/lunaclient/bin/
 2. Select Lunacm: ./lunacm
- ii. To add members in hagroup we need to create a new group on the client
 - haGroup creategroup -serialNumber <serial number> -l <label> -p <password>
 - e.g : lunacm:>haGroup creategroup -serialNumber 1047740028310 -l HAHSM3 -p S@fenet123
- iii. Use the hagroup addmember command to add new member into hagroup client, which requires:
 1. Label for the group (do NOT call the group just "HA").
 2. - the Serial number of the first partition OR the slot number of the first partition.
 3. the password for the partition.
 4. Lunacm also generates and assigns a Serial Number to the group itself
 5. hagroup addMember -group <groupname> -serialNumber <serial number> -password <password>
 - e.g lunacm:>hagroup addMember -group rkmsgroup -serialNumber 1047749341551 -password S@fenet123
- iv. Use the hagroup addmember command to add another member to the HA group.
 - hagroup addMember -group <groupname> -serialNumber <serial number> -password <password>
 - e.g lunacm:>hagroup addMember -serialNumber 1047740028310 -g rkmsgroup -password S@fenet123
- v. Check group member in group using "hagroup listGroups" command.
 - e.g lunacm:>hagroup listGroups
- vi. Enable HAOnly :
 - e.g lunacm:>hagroup HAOnly -enable
- vii. Enable synchronization of HAgrou Members
 - hagroup synchronize -group <groupname> -password <password> -enable
 - e.g lunacm:>hagroup synchronize -group rkmsgroup -password S@fenet123 -enable

b. Version 5

- Client software for HSM Version 5 :

- a. After creating partitions on (at least) two Luna appliances, and setting up NTLS between those partitions and your client, use LunaCM to configure HA on your client.
 - i. Go to directory: /usr/safenet/lunaclient/bin/
- b. To add members in haadmin we need to create a new group on the client.
 - ./vtl haAdmin newGroup -serialNum <HA Group Number> -label <Groupname> -password <password>
 - e.g ./vtl haAdmin newGroup -serialNum 156453092 -label myHAGroup -password S@fenet123
- c. To add members into your haadmin.
 - ./vtl haAdmin addMember -group <HA Group Number> -serialNum <serial_number> -password <password>
 - eg ./vtl haAdmin addMember -group 1156453092 -serialNum 156451030 -password S@fenet123
- d. Enable synchronization of HAadmin Members.
 - ./vtl haAdmin synchronize -group <HA Group Number> -password <password>
 - e.g eg ./vtl haAdmin synchronize -enable -group 1156453092 -password S@fenet123
- e. To Enable HAOnly.
 - ./vtl haAdmin HAOnly -enable
- f. Check haadmin status after synchronization.
 - ./vtl haAdmin show

Note: 1. After synchronization please verify kms master key copied to both partitions registered in hsm ha group. It takes time to copy master key to another partition.

• Installation of Ranger KMS HSM HA

- After configuring HSM HA, to run Ranger KMS in HSM HA mode just we need to specifying the virtual group name create above in "HSM_PARTITION_NAME" property of install.properties and setup and start Ranger KMS.
- Note:** All other configuration for HSM in "install.properties" of Ranger KMS as mentioned in "Installing Ranger KMS HSM" will remain the same.

• Migration

HSM to Ranger DB

1. Stop the Ranger KMS server if running.
2. Go to Ranger KMS directory. eg: /usr/hdp/<version>/ranger-kms

Note: DB details should be proper (in xml config file of Ranger KMS) to which KMS needs migration to.
3. Run: ./HSMK2DB.sh <provider> <HSM_PARTITION_NAME>
 - e.g : ./HSMK2DB.sh LunaProvider par19
4. Enter the partition password.
5. After the migration is completed if you want to run Ranger KMS according to the new configuration (either with HSM enabled or disabled) update the Ranger KMS properties if required.
6. Start Ranger KMS.

Note : After Migration when Ranger KMS is up and running fine with HSM disabled, from HSM clear the Master Key object from the partition if it's not required as Master Key already being migrated to DB.

Ranger DB to HSM

1. Stop the Ranger KMS server if running.
2. Go to Ranger KMS directory. eg: /usr/hdp/<version>/ranger-kms

Note:

 - > DB details from which Ranger KMS needs migration should be proper. (in xml config file of Ranger KMS)
 - > HSM details should be the KMS HSM to which we are migrating to.

3. Run: `./DBMK2HSM.sh <provider> <HSM_PARTITION_NAME>`

e.g : `./DBMK2HSM.sh LunaProvider par19`

4. Enter the partition password.

5. After the migration is completed if you want to run Ranger KMS according to the new configuration (either with HSM enabled or disabled) update the Ranger KMS properties if required.

6. Start Ranger KMS

Note: After Migration when Ranger KMS is up and running fine with HSM enabled, from DB table "ranger_masterkey" delete the Master Key row if it's not required as Master Key already being migrated to HSM.

• Clear Objects from HSM partition

1. SSH to the HSM Appliance Server

- E.g : `ssh admin@elab6.safenet-inc.com`

<Enter Password for HSM Appliance Server when prompted>

2. Check the Partition Objects which you want to clear, command is

- Partition `showContents -par <partition_name>`

- E.g : `partition showContents -par par14`

<Enter Password for Partition when prompted>

Note: Please make it sure after step 3 all objects listed from the above command will get destroyed.

3. Clear the objects from HMS partition using following command

- Partition `clear -par <partition_name>`

<Enter Password for Partition when prompted>

<proceed when prompted>

- E.g : `partition clear -par par14`