Cloudera Manager 7.11.3

Migrating keys from KTS to Ranger KMS

Date published:
Date modified:

CLOUDERA

Legal Notice

Contents

Migrating keys from Key Trustee Server to Ranger KMS

You can migrate keys from Key Trustee Server to Ranger KMS DB.

Important considerations before migrating the keys.

Ranger KMS KTS keys are case sensitive but Ranger KMS DB keys are case insensitive. This means, it is possible to have the following keys in KMS KTS:

- KEY1 // All in capital case
- key1 // All in small case
- Key1 // Mix of both

KMS DB always stores the key names in lower case, even if you provide the key name in uppercase.It will error out when attempting to create duplicate keys with different cases. During Hadoop key migration, this may cause issues. For instance, only one of key listed above will be imported.

Impact:

- Scenario 1: If you have a combination of such keys (with different cases) , only one key will be migrated. The migration tool will ignore the other keys.
- Scenario 2: If you have keys in any cases but no duplicates ,then after migration it will be stored in lowercase and will be visible on UI in lowercase.

Therefore, it is important to check the case of the keynames before starting the migration.

Key migration

This procedure describes how to migrate keys from Key Trustee Server to Ranger KMS.

Before you begin

- Locate the keys in Key Trustee Server.

  - Login to Ranger UI with Key Admin credentials.
  - Go to Key Management -> Select Service , to view the HDFS encryption zone keys with service Ranger KMS KTS

- If NavEncrypt is setup, locate its keys.

  - SSH in to the active KTS node.
  - Login to Postgres 14 database for 7.1.9 , or to Postgres 12 database for CDP versions 7.1.8 and less.
  - The 'keytrustee' user is created with 'nologin' by default. Update the keytrustee user in /etc/passwd before accessing the database by running the following command:

```
sed -i "/keytrustee:x:$( id -u keytrustee ):$( id -g keytrustee ):Keytru
stee User:\/var\/lib\/keytrustee:\/sbin\/nologin/c\keytrustee:x:$( id -u
 keytrustee ):$( id -g keytrustee ):Keytrustee User:\/var\/lib\/keytrust
ee:\/bin\/bash" /etc/passwd
```

  - Run the following commands :

```
select handle from deposit;
```

For CDP version 7.1.9 :

```
# sudo -u keytrustee LD_LIBRARY_PATH=/opt/cloudera/parcels/KEYTRUSTEE_SE
RVER/PG_DB/opt/postgres/14.2/lib /opt/cloudera/parcels/KEYTRUSTEE_SERVER
/PG_DB/opt/postgres/14.2/bin/psql -p 11381 keytrustee

keytrustee=# select handle from deposit;
handle
---------
mykey1
mykey2

control

control
```

```
(6 rows)
```

For CDP versions less than 7.1.9 :

```
# sudo -u keytrustee LD_LIBRARY_PATH=/opt/cloudera/parcels/KEYTRUSTEE_SE
RVER/PG_DB/opt/postgres/12.1/lib /opt/cloudera/parcels/KEYTRUSTEE_SERVER
/PG_DB/opt/postgres/12.1/bin/psql -p 11381 keytrustee


 keytrustee=# select handle from deposit;
 handle
 ---------
 mykey1
 mykey2

 control

 control
 (6 rows)
```

Procedure

1. Backup the KTS database.
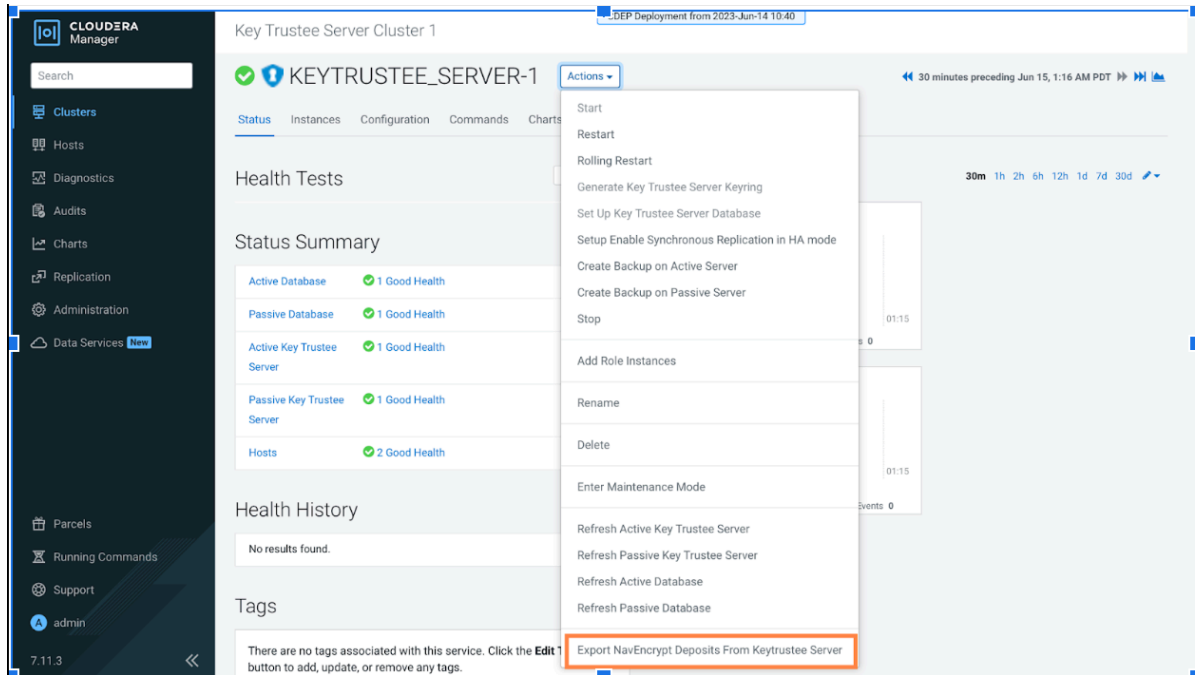
The backup will be created at /var/lib/keytrustee/ on Active KTS node.

2. Export the NavEncrypt keys.

   a) Go to Cloudera Manager Key Trustee Server Click on Actions Export NavEncrypt Deposits from Keytrustee Server

This will generate the CSV required to import NavEncrypt keys in Ranger KMS DB after migration. The deposits.csv file will be created at /var/lib/keytrustee/.keytrustee.

3. Back up the Ranger KMS KTS directory and generate a keystore file of existing encryption zone keys.

The keystore file is protected using Store password (default value : mystorepass) and Key password (default value : mykeypass),that are configurable in RANGER KMS KTS configuration.
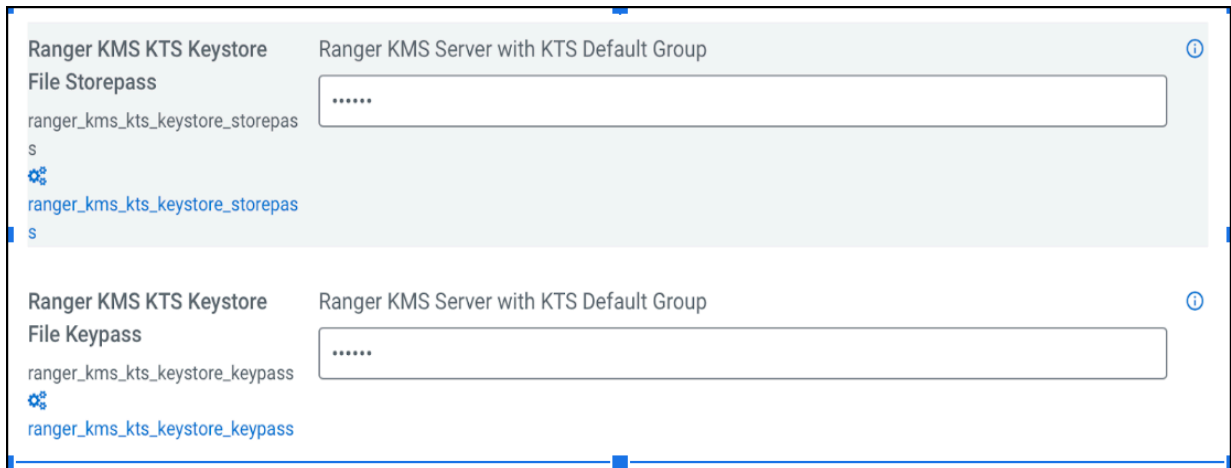
> **Note:** Record the key password and store password as they are required after migration while importing keys in Ranger KMS DB

a) Go to Cloudera Manager Ranger KMS KTS Actions and select Export keys from Ranger KMS KTS
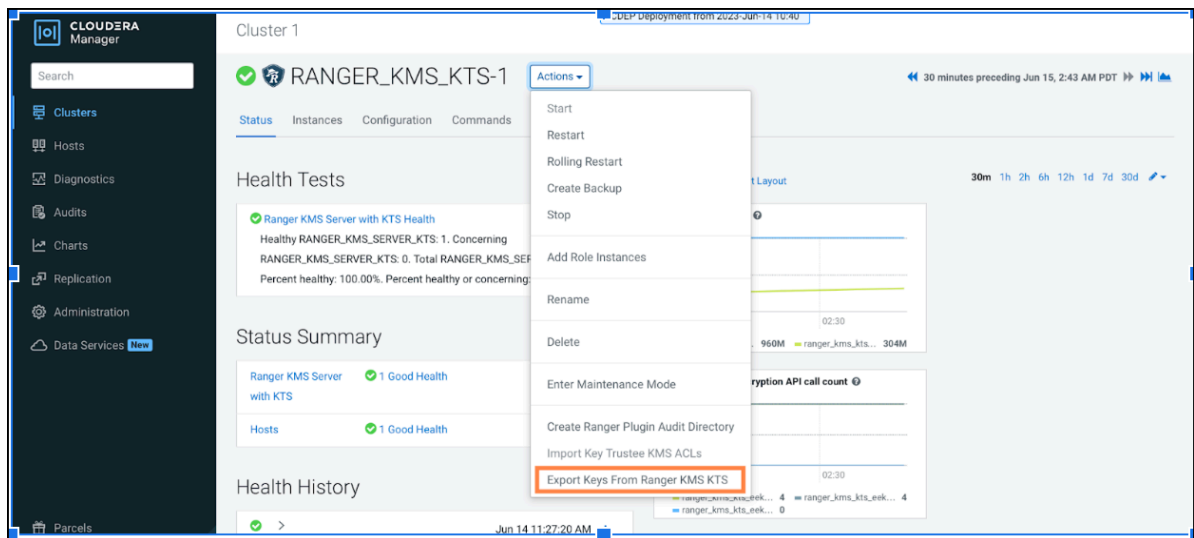
The service GPG keys backup and keystore file will be created at /var/lib/kms-keytrustee on Ranger KMS KTS node.

4. Stop HDFS and Ranger KMS KTS.

5. Delete the Ranger KMS KTS service from CM UI.

6. Add the Ranger KMS service from CM UI and follow the steps as per wizard. For more info, see related links for 'Configuring a database for Ranger or Ranger KMS' and 'Installing Ranger KMS backed by a Database and HA'

7. Enable the migration flag and complete the wizard.

   a) Go to Cloudera Manager Ranger KMS Configuration and check Enable Ranger KMS KTS Migration.
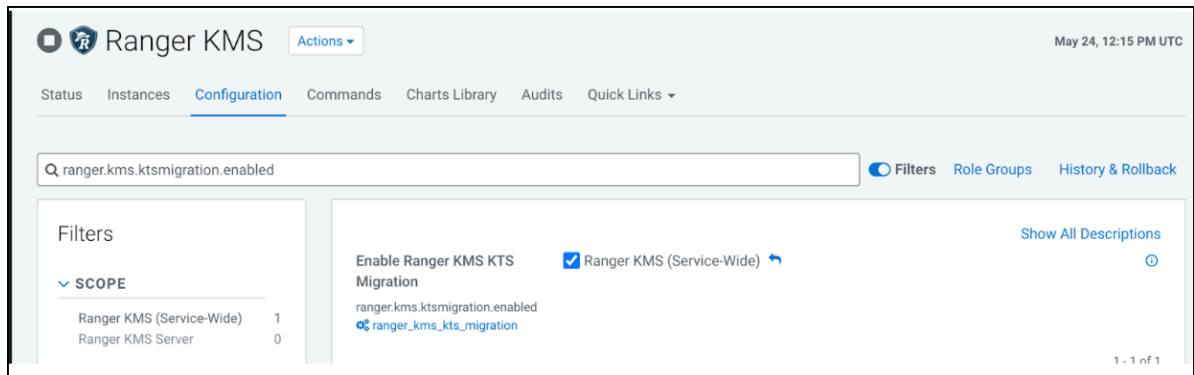
8. Configure the Key password (default value : mykeypass) and Store password (default value : mystorepass) in Ranger KMS configuration.

   These are the same passwords that were configured in Step 3 in Ranger KMS KTS.
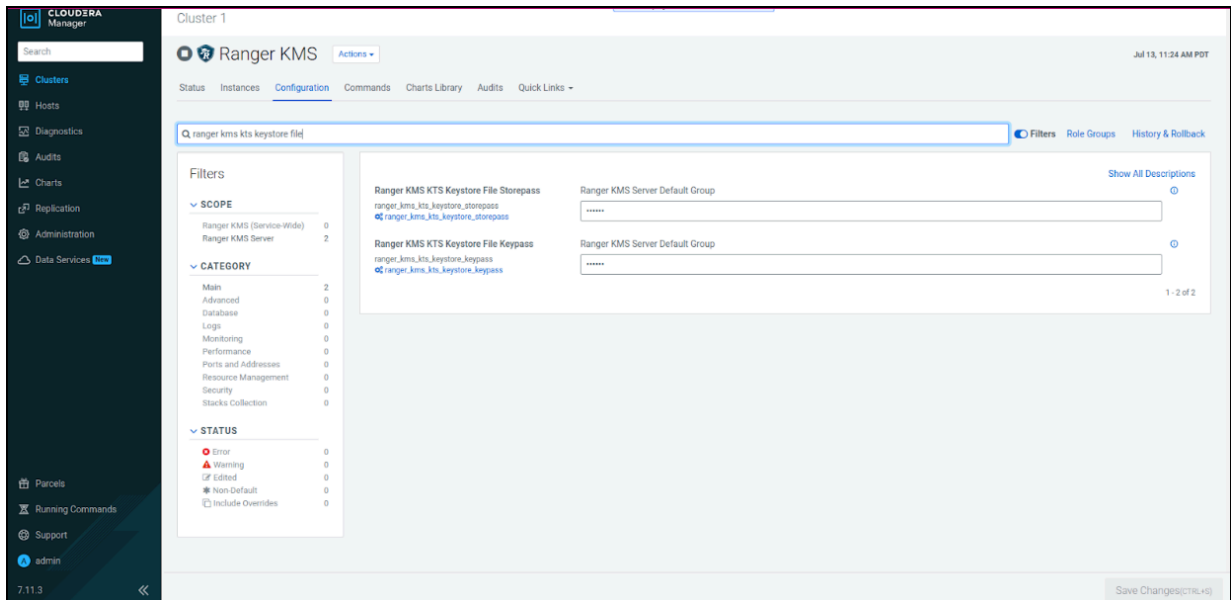
9. If NavEncrypt is configured on the cluster, copy deposits.csv file to the Ranger KMS node, and grant permission kms:kms.

   The location is configurable using the property Key Trustee   NavEncrypt Keys Full Path.
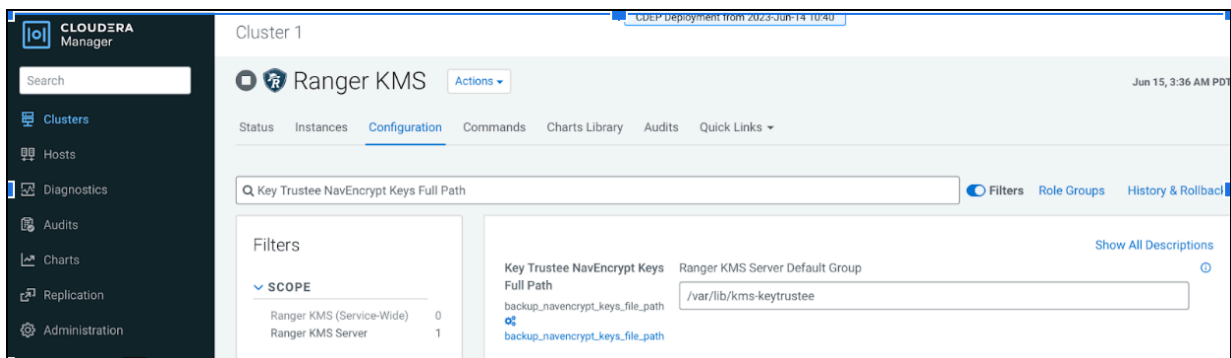

```
 # scp root@dsktstokms-4.vpc.cloudera.com:/var/lib/keytrustee/.keytrustee/
deposits.csv /var/lib/kms-keytrustee
```

```
            100%   10KB   8.2MB/s   00:00
 # ls -ltr /var/lib/kms-keytrustee/deposits.csv
 -rw-r--r-- 1 root root 10401 Jun 15 03:34 /var/lib/kms-keytrustee/depos
its.csv
 # chown kms:kms /var/lib/kms-keytrustee/deposits.csv
 # ls -ltr /var/lib/kms-keytrustee
 total 64
 -rw-r--r-- 1 kms kms 20480 Jun 14 11:22 kms_bak_dsktstokms-3_vpc_cloude
ra_com_2023-06-14_11-22-42.tar
 -rw-r--r-- 1 kms kms   352 Jun 14 11:22 kt_bak_dsktstokms-3_vpc_cloudera
_com_2023-06-14_11-22-42.log
 -rw-r--r-- 1 kms kms 20480 Jun 15 03:20 kms_bak_dsktstokms-3_vpc_cloud
era_com_2023-06-15_03-20-54.tar
 -rw-r--r-- 1 kms kms   352 Jun 15 03:20 kt_bak_dsktstokms-3_vpc_clouder
a_com_2023-06-15_03-20-54.log
  drwxr-xr-x 3 kms kms    55 Jun 15 03:21 keytrustee
 -rw-r--r-- 1 kms kms 10401 Jun 15 03:34 deposits.csv
```

If you want to migrate the KMS hosts, then also copy the migratedKeyStore.jceks file to the Ranger KMS node.

```
 # scp root@dsktstokms-4.vpc.cloudera.com:/var/lib/keytrustee/.keytrustee/
migratedKeyStore.jckes /var/lib/kms-keytrustee/keytrustee

 #ls -ltr /var/lib/kms-keytrustee/keytrustee
  -rw-r--r-- 1 kms kms  1210 Jun 15 03:21 migratedKeyStore.jceks
```

10. Start Ranger KMS.
11. Import the keys from the keystore file and deposits.csv file for NavEncrypt.
    a) Go to Cloudera Manager Ranger KMS Actions and select Import Keys from KTS.

12. Restart Ranger KMS.
13. Start HDFS from CM UI.
14. Stop the Key Trustee Server from CM UI.

> **Note:** Do not remove KTS from Cloudera Manager UI.

Results
After the keys are successfully imported, the keys are visible on Ranger UI.
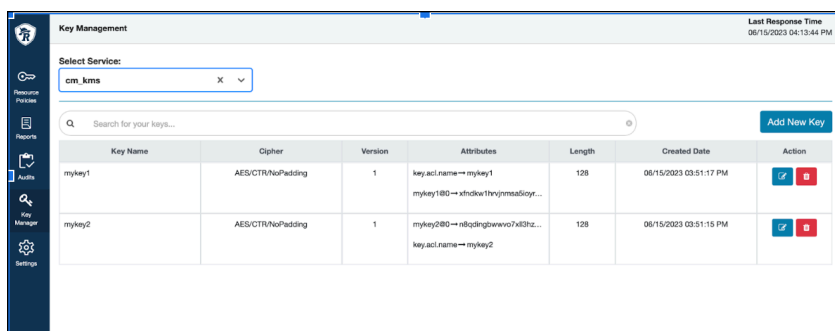
The NavEncrypt keys will be visible in Ranger KMS DB.

```
# mysql -u root -p

MariaDB [(none)]> use rangerkms;

MariaDB [rangerkms]> show tables;
                +--------------------+
                | Tables_in_rangerkms |
                +--------------------+
                | navencrypt_deposit  |
                | ranger_keystore     |
                | ranger_masterkey    |
                +--------------------+
                3 rows in set (0.00 sec)
```

Related Information

Configuring a database for Ranger or Ranger KMS

Installing Ranger KMS backed by a Database and HA

Updating Navigator Encrypt

You must update NavEncrypt to version 7.1.9 in order for it to work with Ranger KMS.

About this task

Learn how to update RHEL compatible Navigator Encrypt. For information on SLES and Ubuntu compatible Navigator Encrypt installation, refer to 'Installing Cloudera Navigator Encrypt'.

Procedure

1. SSH as root to the host where NavEncrypt is installed.
2. Untar the new zip package.

```
tar zxvf navigator-encrypt-7.1.9.0-64-redhat8.tar.gz --directory navencr
ypt-7.1.9.0-repo
```

3. Stop NavEncrypt.

```
systemctl stop navencrypt-mount
```

4. Make a copy of /etc/navencrypt/.

```
cp -rp /etc/navencrypt/ .
```

5. Create, and edit repo file etc/yum.repos.d/navencrypt-7.1.9.0.repo, by adding the following lines.

```
[navencrypt-7.1.9.0]
name=navencrypt-7.1.9.0
baseurl=file:///root/navencrypt-7.1.9.0-repo
gpgkey=file:///root/navencrypt-repo/nepub.asc
enabled=1
gpgcheck=1
```

6. Ensure that the repository is accepted, and three packages are present.

```
# yum repolist
# yum list available --disablerepo=* --enablerepo=navencrypt-7.1.9.0
```

7. Edit the /etc/navencrypt/keytrustee/ztrustee.conf file and make the following changes:

- Change all the URLs to point to Ranger KMS.
- Change "PROTOCOL" to "json-cleartext".
- Add "IS_KMS": true

This is an example of a ztrustee.conf with KTS urls and port :

```
[root@gsne-2 navencryptFiles]# cat /etc/navencrypt/keytrustee/ztrustee.c
onf
{
        "LOCAL_FINGERPRINT": "2048R/51E9DD52660E134E74ECBA8AF0E1ED9AC6AC3B
C9",
        "REMOTES":    {
                "kts1.cloudera.com": {
                        "REMOTE_SERVER": "https://kts1.cloudera.com:11371"
,
                        "HKP_PORT":  11371,
                        "HKP_SCHEME":    "https",
                        "DEFAULT":    true,
                        "HKP_TIMEOUT":  60,
                        "REMOTE_SERVERS": ["https://kts1.cloudera.com:1137
1", "https://kts2.cloudera.com:11371"],
                        "SSL_INSECURE": true,
                        "PROTOCOL":   "json-encrypt",
                        }
                }
}
```

This is an example of ztrustee.conf with Ranger KMS urls and port :

```
[root@gsne-2 ~]# cat /etc/navencrypt/keytrustee/ztrustee.conf
{
        "LOCAL_FINGERPRINT": "2048R/51E9DD52660E134E74ECBA8AF0E1ED9AC6AC3
BC9",
        "REMOTES":    {
                "kms1.cloudera.com": {
                        "REMOTE_SERVER": "https://kms1.cloudera.com:9494",
                        "HKP_PORT":  11371,
                        "HKP_SCHEME":    "https",
                        "DEFAULT":    true,
                        "HKP_TIMEOUT":  60,
                        "REMOTE_SERVERS": ["https://kms1.cloudera.com:9494
", "https://kms2.cloudera.com:9494"],
                        "SSL_INSECURE": true,
                        "PROTOCOL":   "json-cleartext",
                        "IS_KMS":     true
                        }
                }
```

```
}
```

8. Update to new versions of NavEncrypt.

```
yum update libkeytrustee
yum update navencrypt-kernel-module
yum update navencrypt
```

9. Start Navigator Encrypt.

```
systemctl start navencrypt-mount
```

10. Check the version and status of NavEncrypt.

```
navencrypt --version;
navencrypt status -m:
navencrypt key --verify --only-keytrustee
```

Results

The version of NavEncrypt is 7.1.9.0. The status shows "navencrypt module is running". After entering the master-passphrase, navencrypt outputs "VALID".

Related Information

Installing Cloudera Navigator Encrypt

Rollback of Ranger KMS DB to KTS

This procedure decsribes how to rollback from Ranger KMS DB to KTS in case of failure during or after key migration.

Before you begin

Note : Any keys created after migration from KTS to Ranger KMS will not be present after rollback.

Procedure

1. Stop Ranger KMS and HDFS from the Cloudera Manager UI.

2. Stop Key Trustee Server

> **Note:** KTS was stopped after the keys were migrated, but not deleted.

3. Delete Ranger KMS service from the Cloudera Manager UI.

4. Add Ranger KMS KTS service from the Cloudera Manager UI.

> **Note:** While adding Ranger KMS KTS, restore the GPG keys backup created during the migration at location /var/lib/kms-keytrustee/keytrustee/.keytrustee/. If the backup files were not deleted while removing Ranger KMS KTS during migration, it will be already present at required location

5. Start Ranger KMS KTS and HDFS from the Cloudera Manager UI.