

Cloudera Manager 7.11.3

Migrating keys from KTS to Ranger KMS

Date published:

Date modified:

CLOUdera

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Migrating keys from Key Trustee Server to Ranger KMS.....	4
Key migration.....	4
Updating Navigator Encrypt.....	12
Rollback of Ranger KMS DB to KTS.....	14

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

Key Name	Cipher	Version	Attributes	Length	Created Date	Action
mykey1	AES/CTR/NoPadding	1	key.acl.name=>mykey1	128	06/15/2023 11:17:10 AM	[edit] [delete]
mykey2	AES/CTR/NoPadding	1	key.acl.name=>mykey2	128	06/15/2023 11:17:19 AM	[edit] [delete]

- 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 }:Keytrustee User:\var\lib\keytrustee:\sbin\nologin\c\keytrustee:x:${ id -u keytrustee }:${ id -g keytrustee }:Keytrustee User:\var\lib\keytrustee:\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_SERVER/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_SERVER/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.

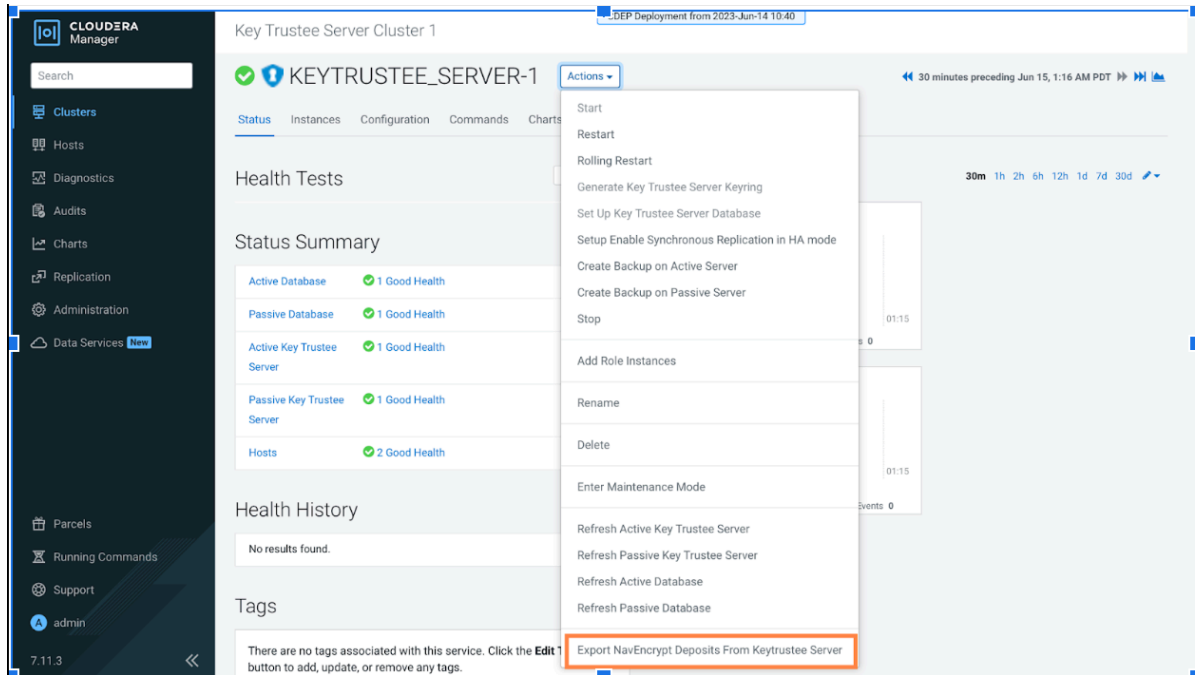
The screenshot shows the Cloudera Manager interface for a node named KEYTRUSTEE_SERVER-1. The 'Actions' dropdown menu is open, displaying various management options. A tooltip for the 'Create Backup' option provides details: 'Create a one-time backup of the keys and the database. Also, adds a cronjob for hourly backups if not present. The backups are stored in the homedir of user keytrustee.' The background interface shows a 'Status Summary' table with the following entries:

Component	Status
Active Database	1 Good Health
Passive Database	1 Good Health
Active Key Trustee Server	1 Good Health
Passive Key Trustee Server	1 Good Health

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



The screenshot displays the Cloudera Manager interface for a Key Trustee Server Cluster. The main content area shows the cluster name 'KEYTRUSTEE_SERVER-1' and a 'Status Summary' table. The 'Status Summary' table lists the following components and their health:

Component	Health
Active Database	1 Good Health
Passive Database	1 Good Health
Active Key Trustee Server	1 Good Health
Passive Key Trustee Server	1 Good Health
Hosts	2 Good Health

The 'Actions' dropdown menu is open, showing various options. The option 'Export NavEncrypt Deposits From Keytrustee Server' is highlighted with a red box.

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

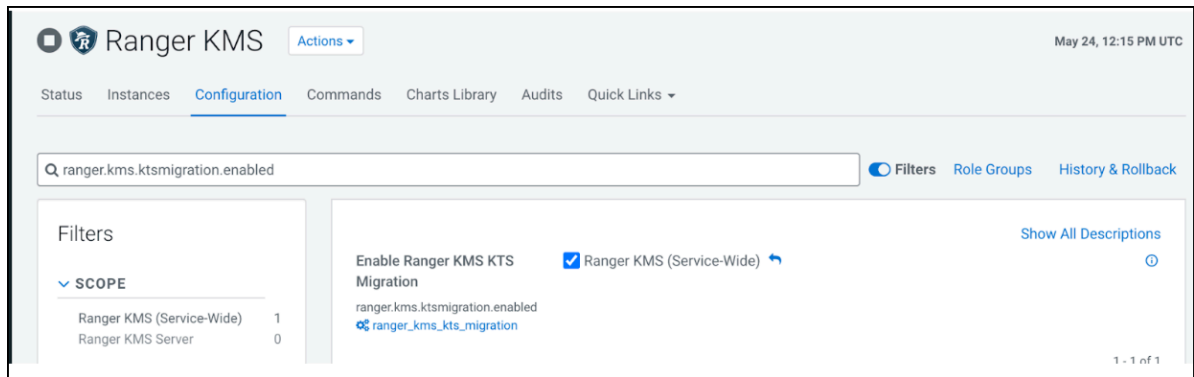
- a) Go to Cloudera Manager Ranger KMS KTS Actions and select Export keys from Ranger KMS KTS

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**.



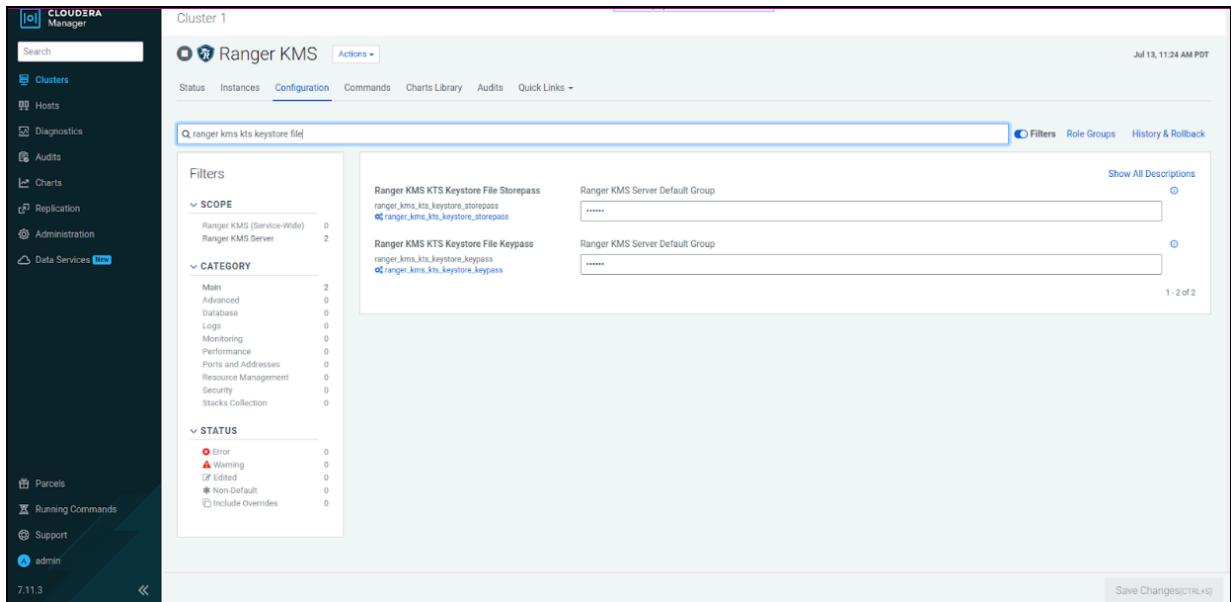
The screenshot shows the 'Ranger KMS' configuration page in Cloudera Manager. The search bar contains 'ranger.kms.ktsmigration.enabled'. Under the 'Filters' section, the 'SCOPE' filter shows 'Ranger KMS (Service-Wide)' with a count of 1. The main configuration area shows the 'Enable Ranger KMS KTS Migration' checkbox is checked, with the label 'Ranger KMS (Service-Wide)'. Below this, the property 'ranger.kms.ktsmigration.enabled' is listed with a link to 'ranger_kms_kts_migration'. The page is dated May 24, 12:15 PM UTC.



Important: You must keep this property enabled even after migration. Disabling this property impacts the encryption zone key retrieval.

8. Configure the Key password (default value : mykeypass) and Store password (default value : mystorepass) in Ranger KMS configuration.

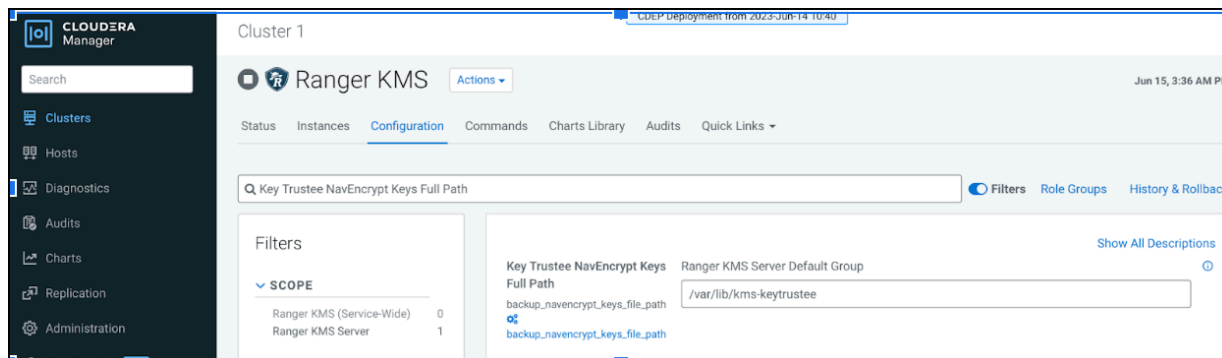
These are the same passwords that were configured in Step 3 in Ranger KMS KTS.



The screenshot shows the 'Ranger KMS' configuration page in Cloudera Manager. The search bar contains 'ranger kms kts keystore file'. The 'Filters' section shows 'SCOPE' with 'Ranger KMS (Service-Wide)' at 0 and 'Ranger KMS Server' at 2. The main configuration area shows two sections: 'Ranger KMS KTS Keystore File Storepass' and 'Ranger KMS KTS Keystore File Keypass'. Each section has a text input field for the password and a dropdown menu for the 'Ranger KMS Server Default Group'. The page is dated Jul 13, 11:24 AM PDT.

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.jckes` file to the Ranger KMS node.

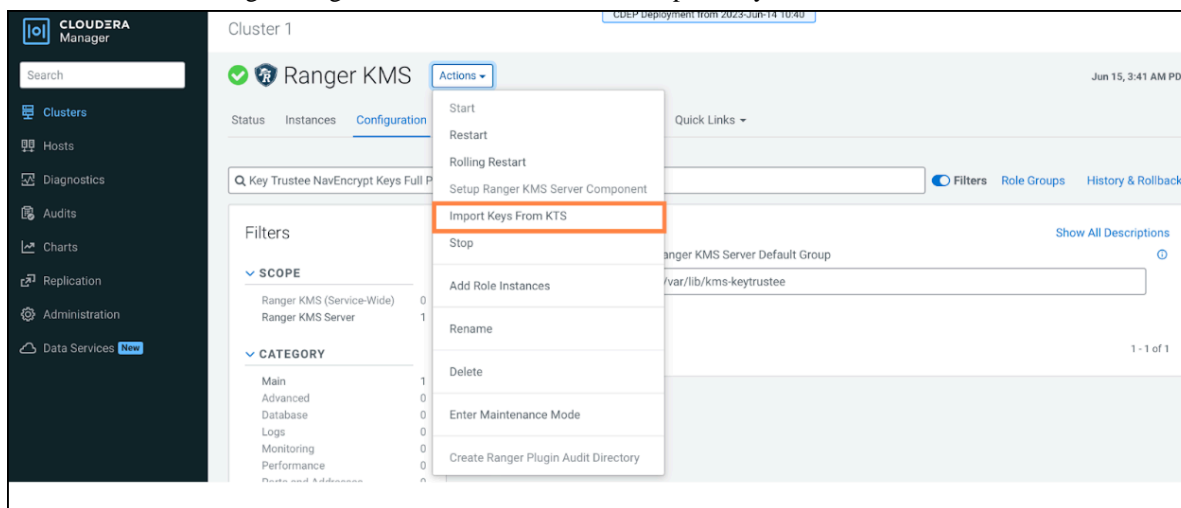
```
# scp root@dsktstokms-4.vpc.cloudera.com:/var/lib/keytrustee/.keytrustee/
migratedKeyStore.jckes /var/lib/kms-keytrustee/keytrustee

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

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 screenshot shows the Ranger Key Management interface. The 'Select Service' dropdown is set to 'cm_kms'. A search bar is present. Below is a table with the following data:

Key Name	Cipher	Version	Attributes	Length	Created Date	Action
mykey1	AES/CTR/NoPadding	1	key.aci.name == mykey1 mykey1@0 == sfndkwtbrymsa@0cy...	128	06/15/2023 03:51:17 PM	[✓] [✗]
mykey2	AES/CTR/NoPadding	1	mykey2@0 == n8p0ngtawwvz7k3hz... key.aci.name == mykey2	128	06/15/2023 03:51:15 PM	[✓] [✗]

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:11371", "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/51E9DD52660E134E74ECBA8AF0E1ED9AC6AC3BC9",
    "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 describes 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.