

## Configuring and Using Ranger KMS

Date published: 2020-07-28

Date modified: 2021-12-13



# 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

<b>Configuring Ranger KMS High Availability.....</b>	<b>4</b>
Configure High Availability for Ranger KMS with DB.....	4
Configure High Availability for Ranger KMS with KTS.....	13

# Configuring Ranger KMS High Availability

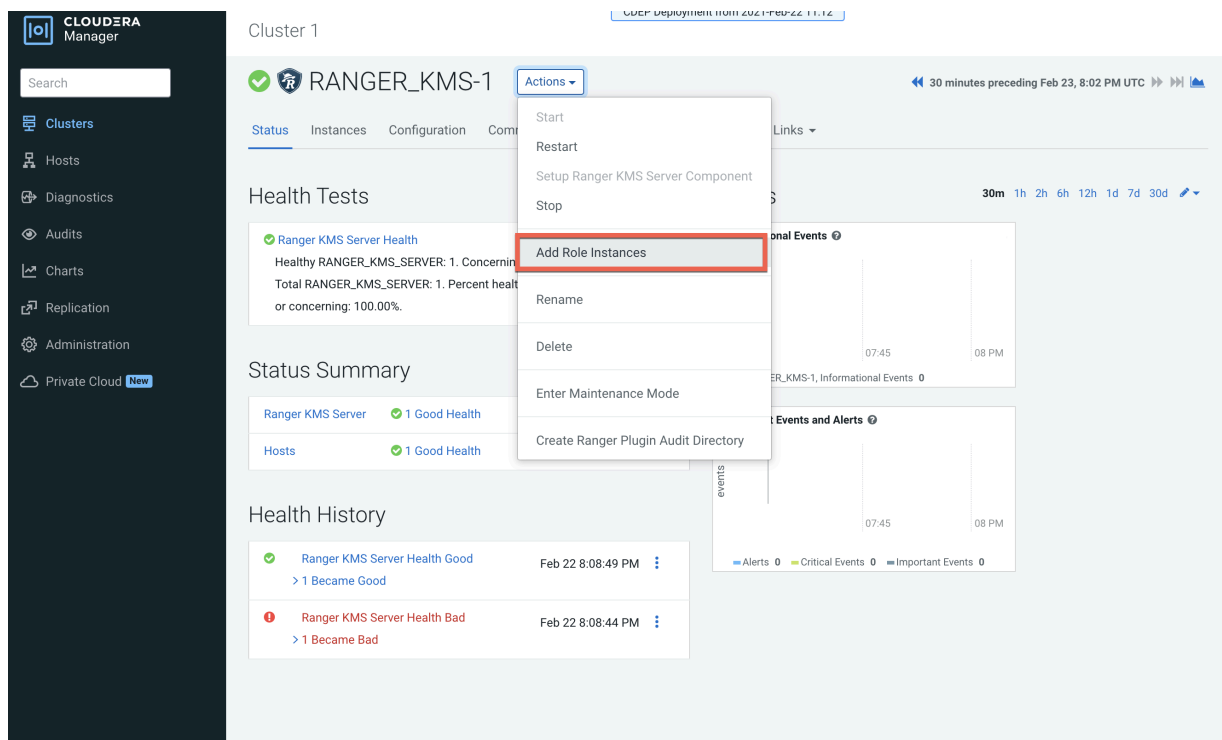
How to configure Ranger KMS high availability (HA) for Ranger KMS.

## Configure High Availability for Ranger KMS with DB

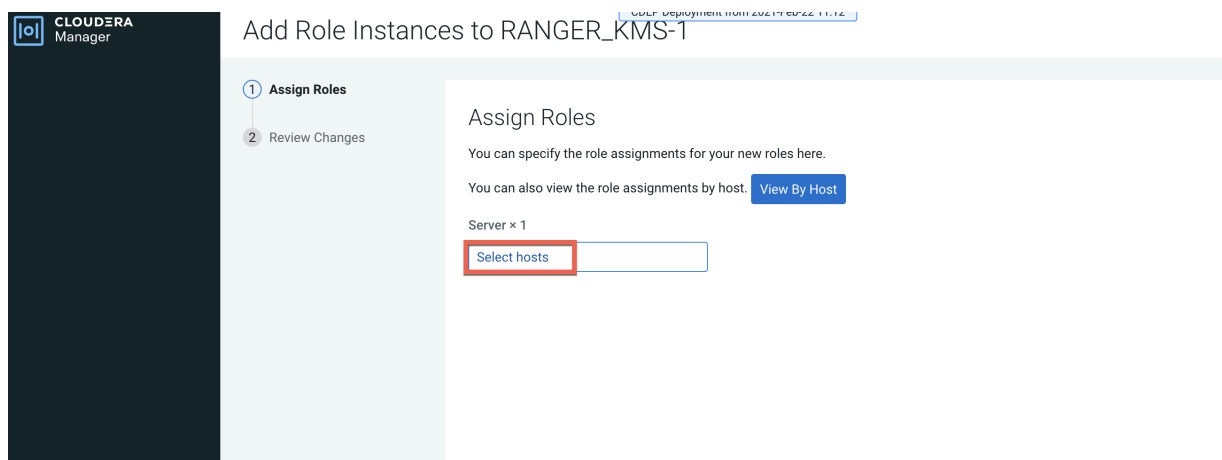
Use the following steps to configure high availability for Ranger KMS with an associated keystore database.

### Procedure

1. In Cloudera Manager, select Ranger KMS, then select Actions > Add Role Instances.



2. On the Assign Roles page, click Select hosts.



- On the selected hosts page, select a backup Ranger KMS host. A Ranger KMS (RK) icon appears in the Added Roles column for the selected host. Click OK to continue.



**Note:** These steps show how to add one additional backup Ranger KMS host, but you can use the same procedure to add multiple Ranger KMS hosts.

2 Hosts Selected

Select hosts for a new or existing role. The host list is filtered to remove hosts that are not valid candidates; these include hosts that are unhealthy, members of other clusters, or have an incompatible version of the software installed on them.

Enter hostnames: host01, IP addresses or rack

<input type="checkbox"/>	Hostname	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
<input checked="" type="checkbox"/>	cloudera71-21name	172.27.0.69	/default	80	251.6 GiB	AS, CCS, G, HB..., RS, DN, G, G, G, ID, KB, KC, KG, M, L, G, LS, RA, RT, RU, RK..., SRS, G, G, SM..., SR..., SR..., G, G, NM, ZS	RK...
<input checked="" type="checkbox"/>	cloudera71-21name	172.27.0.71	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, L, G, G, G, SR..., G, NM	RK...
<input type="checkbox"/>	cloudera71-21name	172.27.0.12	/default	32	251.6 GiB	M, B, NN, NF..., SNN, G, HMS, G, HS2, LB, HS, KTR, ICS, ISS, G, KB, KC, LHBI, TS, L, G, AP, ES, HM, RM, SM, OS, SS, G, HS, G, G, JHS, RM, S	

1 - 3 of 3

Cancel OK

- The Assign Roles page is redisplayed with the new backup host. Click Continue.

Add Role Instances to RANGER\_KMS-1

1 Assign Roles

2 Review Changes

Assign Roles

You can specify the role assignments for your new roles here.

You can also view the role assignments by host. [View By Host](#)

Server x (1 + 1 New)

cloudera71-21name & cloudera71-21name3.ro...

Back Continue

5. Review the settings on the Review Changes page, then click Continue.

1 Assign Roles

2 Review Changes

### Review Changes

<b>Ranger KMS Master Key Password</b> ranger.db.encrypt.key.password <a href="#">ranger_kms_master_key_password</a>	<b>Ranger KMS Server Default Group</b> .....	0
<b>Ranger KMS DB Auth Type</b> ranger.ks.db.ssl.auth.type <a href="#">ranger_ks_db_ssl_auth_type</a>	<b>Ranger KMS Server Default Group</b> <input checked="" type="radio"/> 1-way <input type="radio"/> 2-way	0
<b>Ranger KMS Database SSL Certificate File</b> ranger.ks.db.ssl.certificateFile <a href="#">ranger_ks_db_ssl_certificateFile</a>	<b>Ranger KMS Server Default Group</b> 	0
<b>Ranger KMS DB SSL Enabled</b> ranger.ks.db.ssl.enabled <a href="#">ranger_ks_db_ssl_enabled</a>	<input type="checkbox"/> Ranger KMS Server Default Group	0
<b>Ranger KMS DB SSL Required</b> ranger.ks.db.ssl.required <a href="#">ranger_ks_db_ssl_required</a>	<input type="checkbox"/> Ranger KMS Server Default Group	0
<b>Ranger KMS DB SSL Verify Server Certificate</b> ranger.ks.db.ssl.verifyServerCertificate <a href="#">ranger_ks_db_ssl_verifyServerCertificate</a>	<input type="checkbox"/> Ranger KMS Server Default Group	0
<b>Ranger KMS Keystore File</b> ranger.ks.keystore.file <a href="#">ranger_ks_keystore_file</a>	<b>Ranger KMS Server Default Group</b> 	0
<b>Ranger KMS Keystore Password</b> ranger.ks.keystore.password <a href="#">ranger_ks_keystore_password</a>	<b>Ranger KMS Server Default Group</b> 	0
<b>Ranger KMS Truststore File</b> ranger.ks.truststore.file <a href="#">ranger_ks_truststore_file</a>	<b>Ranger KMS Server Default Group</b> 	0

Parcels

Running Commands

Support

admin

7.3.0

Back

Continue

- CLUSTER DEPLOYMENT FROM 2021-02-22 11:12

CLUSTER: RANGER\_KMS-1

Actions

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Private Cloud New

Status

Instances

Configuration

Commands

Charts Library

Audits

Quick Links

**This entity is currently running with an outdated configuration. Restart the service (or the instance) for the changes to take effect.**

Search

Filters

Last Updated: Feb 23, 8:24:09 PM UTC

Filters

STATUS

Stopped 1

Good Health 1

COMMISSION STATE

MAINTENANCE MODE

RACK ID

ROLE GROUP

ROLE TYPE

STATE

HEALTH TEST

Actions for Selected

Add Role Instances

Role Groups

<input type="checkbox"/>	Status	Role Type	State	Hostname	Commission State	Role Group
<input type="checkbox"/>		Ranger KMS Server	Stopped	10.10.10.10	Commissioned	Ranger KMS Server Default Group
<input type="checkbox"/>		Ranger KMS Server	Started with Outdated Configuration	10.10.10.10	Commissioned	Ranger KMS Server Default Group

1 - 2 of 2

7. In Cloudera Manager, select the Ranger service, click Ranger Admin Web UI, then log in as the Ranger KMS user (the default credentials are keyadmin/admin123). Click the Edit icon for the cm\_kms service, then update the KMS URL property.

- Add the new KMS host using the following format:  
kms://http@<kms\_host1>;http@<kms\_host2>:<kms\_port>/kms
- The default port is 9292. For example:  
kms://http@kms\_host1;http@kms\_host2:9292/kms
- If SSL is enabled, use https and port 9494. For example:  
kms://http@kms\_host1;https@kms\_host2:9494/kms

Click Test Connection to confirm the settings, then click Save to save your changes.

The screenshot shows the 'Edit Service' page for the 'cm\_kms' service in the Ranger Admin Web UI. The page is divided into two main sections: 'Service Details' and 'Config Properties'.

**Service Details:**

- Service Name:** cm\_kms
- Display Name:** cm\_kms
- Description:** KMS repo
- Active Status:** ☒ Enabled ☐ Disabled
- Select Tag Service:** Select Tag Service

**Config Properties:**

- KMS URL:** it.hwx.site;http@...:9292/kms-2.d...:9292/kms.root.hwx
- Username:** keyadmin
- Password:** .....

**Add New Configurations:**

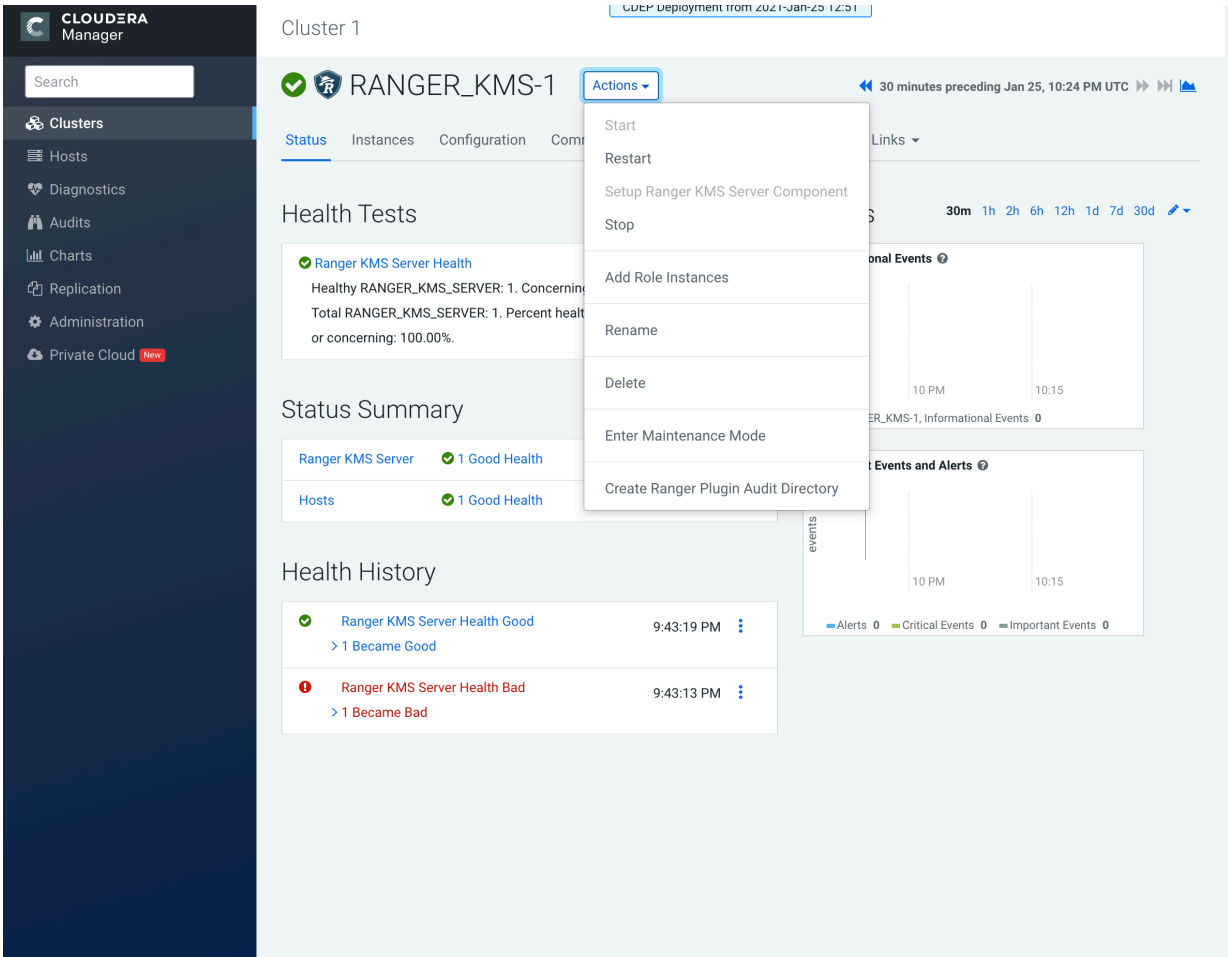
Name	Value	
cluster.name	Cluster 1	<input type="button" value="x"/>
policy.download.auth.users	keyadmin,rangerkms	<input type="button" value="x"/>

Below the table is a '+' button to add more configurations.

At the bottom of the page, there is a 'Test Connection' button and a row of buttons: 'Save', 'Cancel', and 'Delete'.



8. In Cloudera Manager click the Ranger KMS service, then select Actions > Create Ranger Plugin Audit Directory.



9. In Cloudera Manager, select Ranger KMS, then click Configuration.

a) Use the Add (+) icons for the Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml property to add the following properties, then click Save Changes.

- `hadoop.kms.authentication.zk-dt-secret-manager.enable = true`
- `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <Zookeeper hostname>:2181`



**Note:** In a cluster with multiple ZK hosts, include them as a comma-separated list.  
For example: `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <ZK_hostname1>:2181,<ZK_hostname2>:2181,....,<ZK_hostnameN>:2181`.

- `hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = <provide a znode working path other than /zkdt-sm to avoid collision>`

For example:

`hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = testzkms`



**Note:** Do not put a leading slash at the beginning of the znode working path.

- `hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType = sasl`
- `hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab = {{CMF_CONF_DIR}}/ranger_kms.keytab`

The screenshot shows the Cloudera Manager interface for configuring Ranger KMS. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area is titled 'Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml'. It features a 'Filters' panel on the left with sections for SCOPE, CATEGORY, and STATUS. The main panel displays a list of configuration properties with their names, values, and descriptions. The properties are:

- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.enable`, **Value:** `true`, **Description:** (empty)
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString`, **Value:** `hwx.site:2181`, **Description:** (empty)
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath`, **Value:** `testzkms`, **Description:** (empty)
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType`, **Value:** `sasl`, **Description:** (empty)
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab`, **Value:** `{{CMF_CONF_DIR}}/ranger_kms.keytab`, **Description:** (empty)

At the bottom, there is a status bar indicating '1 Edited Value' and a 'Reason for change' field. A 'Save Changes (CTRL+S)' button is located at the bottom right.

10. Update the following Ranger KMS configuration properties, then click Save Changes.

- `hadoop.kms.authentication.signer.secret.provider = zookeeper`
- `hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type = sasl`

Cluster 1

CDEP Deployment from 2021-Feb-22 11:12

RANGER\_KMS-1

Feb 25, 7:06 PM UTC

Status Instances **Configuration** Commands Charts Library Audits Quick Links

Q `hadoop.kms.authentication.signer.secret.provider` Filters Role Groups History and Rollback

**Filters**

SCOPE

- RANGER\_KMS-1 (Service-Wide) 0
- Ranger KMS Server 3

CATEGORY

- Advanced 0
- Database 0
- Logs 0
- Main 3
- Monitoring 0
- Performance 0
- Ports and Addresses 0
- Resource Management 0
- Security 0
- Stacks Collection 0

STATUS

- Error 0
- Warning 0
- Edited 2
- Non-default 2
- Has Overrides 0

**Hadoop KMS Authentication Signer Secret Provider**

hadoop.kms.authentication.signer.secret.provider

hadoop\_kms\_authentication\_signer\_secret\_provider

Ranger KMS Server Default Group [Undo](#)

☐ random

☐ string

☒ zookeeper

**Hadoop KMS Authentication Signer Secret Provider Zookeeper Path**

hadoop.kms.authentication.signer.secret.provider.zookeeper.path

hadoop\_kms\_authentication\_signer\_secret\_provider\_zookeeper\_path

Ranger KMS Server Default Group [Undo](#)

**Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type**

hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type

hadoop\_kms\_authentication\_signer\_secret\_provider\_zookeeper\_auth\_type

☐ none

☐ kerberos

☒ sasl

Per Page 25 1 - 25 of 142

2 Edited Values Reason for change: Modified Hadoop KMS Authentication Signer Secret Provider, Hadoop KMS Authentication Signer Secret Provider

**Save Changes (CTRL+S)**

11. Verify that the `hadoop.kms.cache.enable` property is set to the default value of `true` (the check box is selected).

CLUSTER

CLUSTER

MANAGER

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Private Cloud New

Parcels

Running Commands

Support

admin

Cluster 1

CDEP Deployment from 2021-Feb-22 11:12

RANGER\_KMS-1

Actions

Feb 25, 9:39 PM UTC

Status

Instances

Configuration

Commands

Charts Library

Audits

Quick Links

hadoop.kms.cache.enable

Filters

Role Groups

History and Rollback

Filters

SCOPE

RANGER\_KMS-1 (Service-Wide) 0

Ranger KMS Server 1

CATEGORY

Advanced 0

Database 0

Logs 0

Main 1

Monitoring 0

Performance 0

Ports and Addresses 0

Resource Management 0

Security 0

Stacks Collection 0

STATUS

Error 0

Warning 0

Edited 0

Non-default 0

Has Overrides 0

Hadoop KMS Cache Enable

hadoop.kms.cache.enable

hadoop\_kms\_cache\_enable

Ranger KMS Server Default Group

Show All Descriptions

Per Page 25

1 - 25 of 142

12

12. Click the Stale Configuration Restart icon.

The screenshot shows the Cloudera Manager interface for Cluster 1. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Private Cloud, Parcels, Running Commands, Support, and a user profile 'admin'. The main panel is titled 'Cluster 1' and shows the 'RANGER\_KMS-1' configuration page. The 'Configuration' tab is selected, and a search bar contains 'hadoop.kms.cache.enable'. A 'Filters' sidebar on the left lists categories: SCOPE (RANGER\_KMS-1 (Service-Wide) 0, Ranger KMS Server 1), CATEGORY (Advanced 0, Database 0, Logs 0, Main 1, Monitoring 0, Performance 0, Ports and Addresses 0, Resource Management 0, Security 0, Stacks Collection 0), and STATUS (Error 0, Warning 0, Edited 0, Non-default 0, Has Overrides 0). A 'Stale Configuration: Restart needed' tooltip is visible over the 'Actions' button. The main content area shows the 'Hadoop KMS Cache Enable' configuration with a checked 'Ranger KMS Server Default Group' checkbox. The bottom right has a 'Save Changes (CTRL+S)' button.

13. On the Stale Configurations page, click Restart Stale Services.

14. On the Restart Stale Services page, select the Re-deploy client configuration checkbox, then click Restart Now.

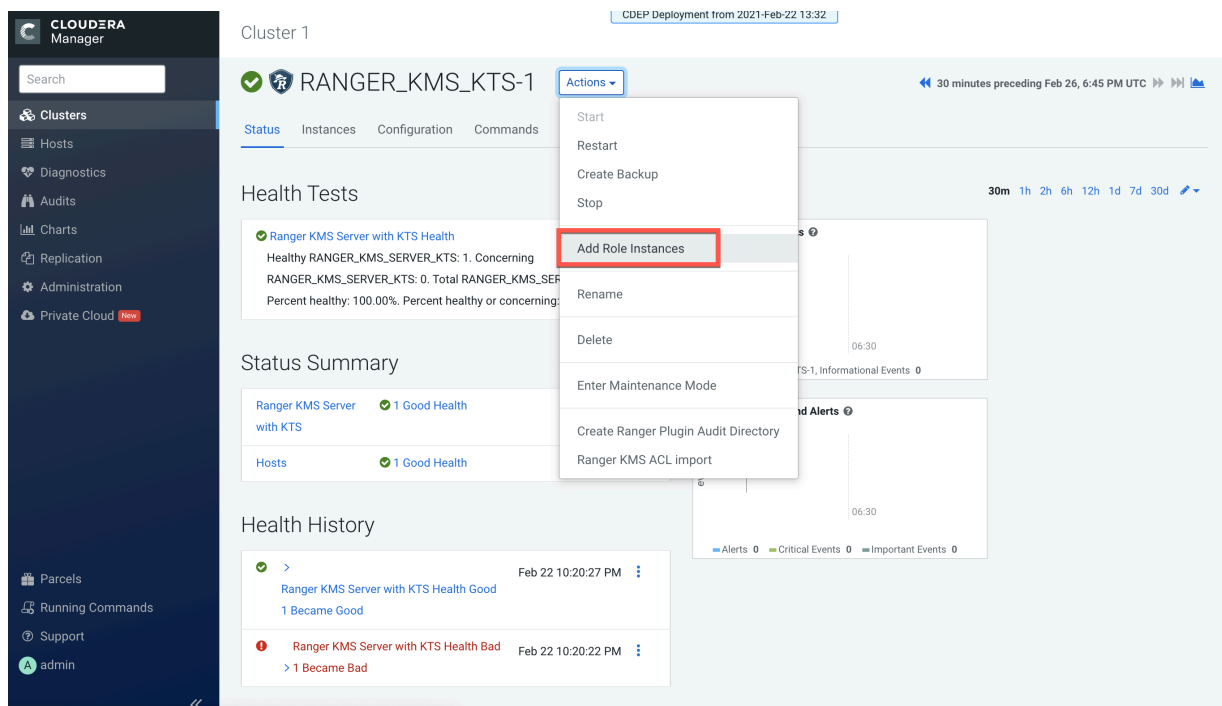
15. A progress indicator page appears while the services are being restarted. When the services have restarted, click Finish.

## Configure High Availability for Ranger KMS with KTS

Use the following steps to configure high availability for Ranger KMS with Key Trustee Server as the backing key store.

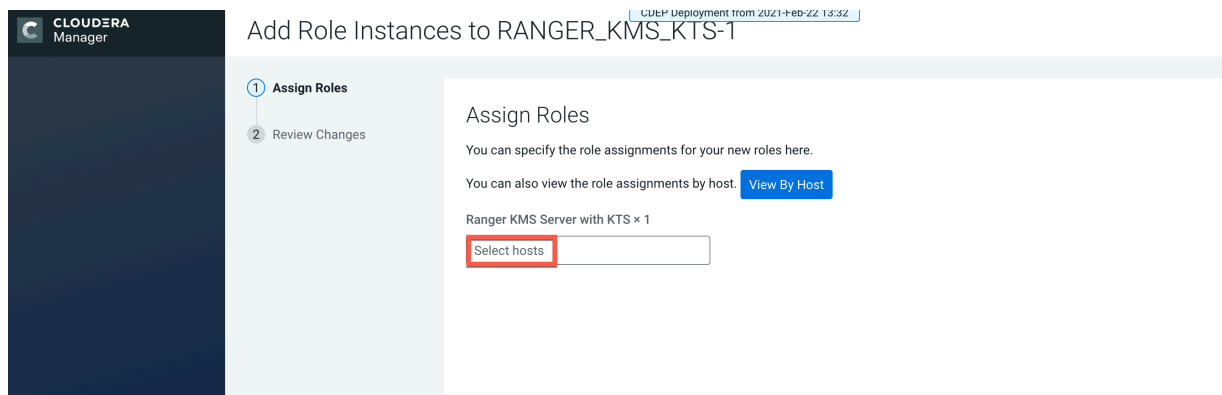
## Procedure

1. In Cloudera Manager, select Ranger KMS KTS, then select Actions > Add Role Instances.



The screenshot shows the Cloudera Manager interface for a cluster named 'RANGER\_KMS\_KTS-1'. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Private Cloud, Parcels, Running Commands, Support, and an admin user. The main panel displays the cluster's status, including Health Tests, Status Summary, and Health History. The 'Actions' dropdown menu is open, showing options like Start, Restart, Create Backup, Stop, Add Role Instances (highlighted with a red box), Rename, Delete, Enter Maintenance Mode, Create Ranger Plugin Audit Directory, and Ranger KMS ACL import.

2. On the Assign Roles page, click Select hosts.



The screenshot shows the 'Assign Roles' page in Cloudera Manager. The page title is 'Add Role Instances to RANGER\_KMS\_KTS-1'. The left sidebar shows the 'Assign Roles' step selected. The main panel contains instructions on how to specify role assignments and a 'View By Host' button. Below this, it shows 'Ranger KMS Server with KTS × 1' and a 'Select hosts' button, which is highlighted with a red box.

- On the selected hosts page, select a backup Ranger KMS KTS host. A Ranger KMS KTS (RK) icon appears in the Added Roles column for the selected host. Click OK to continue.



**Note:** These steps show how to add one additional backup Ranger KMS KTS host, but you can use the same procedure to add multiple Ranger KMS KTS hosts.

2 Hosts Selected

Select hosts for a new or existing role. The host list is filtered to remove hosts that are not valid candidates; these include hosts that are unhealthy, members of other clusters, or have an incompatible version of the software installed on them.

Q Enter hostnames: host01, IP addresses or rack

<input type="checkbox"/>	Hostname	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
<input type="checkbox"/>	dh...71...site	172.27.130.1	/default	32	251.6 GiB	AS, CCS, G, HB..., RS, DN, G, G, G, ID, KB, KC, KG, M, LS, RA, RT, RU, SRS, G, G, SM..., SM..., SR..., SR..., G, G, NM, ZS	
<input checked="" type="checkbox"/>	dh...71...site	172.27.130.71	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, G, RK..., G, G, NM	RK...
<input checked="" type="checkbox"/>	dh...71...site	172.27.130.09	/default	32	503.6 GiB	M, B, NN, NF..., SNN, G, HMS, G, HS2, LB, HS, KTR, ICS, ISS, G, KB, KC, LHBI, TS, G, AP, ES, HM, RM	RK...

Cancel

OK

- The Assign Roles page is redisplayed with the new backup host. Click Continue.

CLUSTER

CLUSTER NAME

CLUSTER STATUS

CLUSTER TYPE

CLUSTER VERSION

CLUSTER ID

1 Assign Roles

2 Review Changes

Add Role Instances to RANGER\_KMS\_KTS-1

CDEP Deployment from 2021-Feb-22 13:32

Assign Roles

You can specify the role assignments for your new roles here.

You can also view the role assignments by host. [View By Host](#)

Ranger KMS Server with KTS × (1 + 1 New)

dh...-3.d...mskts...

Back

Continue

5. Review the settings on the Review Changes page, then click Continue.

CLUSTER Deployment from 2021-Feb-22 13:32

Add Role Instances to RANGER\_KMS\_KTS-1

Assign Roles

2 Review Changes

### Review Changes

Key Trustee Server Auth Code Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.auth .....

Active Key Trustee Server Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.hostname kts-cdep-server-1.vpc.cloudera.com ⓘ

ame-ACTIVE

Passive Key Trustee Server Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.hostname kts-cdep-server-2.vpc.cloudera.com ⓘ

ame-PASSIVE

Key Trustee Server Org Name Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.org kts

Key Trustee Server Key Provider Pool Timeout Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.pool.abandoned.timeout 5 minute(s) v

Key Trustee Server Key Provider Max Connections Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.pool.max 5

Key Trustee Server Key Provider Pool Max Idle Ranger KMS Server with KTS Default Group ⓘ

cloudera.trustee.keyprovider.pool.max.idle 2

Back Continue

6. The new role instance appears on the Ranger KMS KTS page. If the new Ranger KMS with KTS instance was not started by the wizard, you can start the service by clicking Actions > Start in the Ranger KMS with Key Trustee Server service.

CLUSTER Deployment from 2021-Feb-22 13:32

Cluster 1

✓ RANGER\_KMS\_KTS-1

Status Instances Configuration Commands

This entity is currently running with an outdated configuration. (Click here to refresh the configuration) for the changes to take effect.

Last Updated: Feb 26, 7:16:40 PM UTC

Filters

STATUS

Stopped 1

Good Health 1

COMMISSION STATE

MAINTENANCE MODE

RACK ID

ROLE GROUP

ROLE TYPE

STATE

HEALTH TEST

Actions for RANGER\_KMS\_KTS-1

- Start
- Restart
- Create Backup
- Stop
- Add Role Instances
- Rename
- Delete
- Enter Maintenance Mode
- Create Ranger Plugin Audit Directory
- Ranger KMS ACL import

Hostname	Commission State	Role Group
dhoyle715kmskts-3.dhoyle715kmskts.root.hwx.site	Commissioned	Ranger KMS Server with KTS Default Group
dhoyle715kmskts-2.dhoyle715kmskts.root.hwx.site	Commissioned	Ranger KMS Server with KTS Default Group

1 - 2 of 2



7. If necessary, synchronize the KMS KTS private key.

Check the catalina.out file in the Ranger KMS KTS log directory for the following error:

```
java.io.IOException: Unable to verify private key match between KMS hosts.  
Verify private key files have been synced  
between all KMS hosts. Aborting to prevent data inconsistency.
```

To determine whether the KMS KTS private keys are different, compare the MD5 hash of the private keys. On each Ranger KMS KTS host, run the following command:

```
md5sum /var/lib/kms-keytrustee/keytrustee/.keytrustee/secring.gpg
```

If the output is different on both instances, Cloudera recommends following security best practices and transferring the private key using offline media, such as a removable USB drive. For convenience (for example, in a development or testing environment where maximum security is not required), you can copy the private key over the network by running the following rsync command on the original Ranger KMS KTS host:

```
rsync -zav /var/lib/kms-keytrustee/keytrustee/.keytrustee root@kms02.e  
xample.com:/var/lib/kms-keytrustee/keytrustee/.
```

8. Restart the Ranger KMS KTS service.

9. In Cloudera Manager, select the Ranger service, click Ranger Admin Web UI, then log in as the Ranger KMS user (the default credentials are keyadmin/admin123). Click the Edit icon for the cm\_kms service, then update the KMS URL property.

- Add the new KMS host using the following format:  
kms://http@<kms\_kts\_host1>;http@<kms\_kts\_host2>:<kms\_port>/kms
- The default port is 9292. For example:  
kms://http@kms\_kts\_host1;http@kms\_kts\_host2:9292/kms
- If SSL is enabled, use https and port 9494. For example:  
kms://https@kms\_kts\_host1;https@kms\_kts\_host2:9494/kms

Click Test Connection to confirm the settings, then click Save to save your changes.

The screenshot shows the Ranger Admin Web UI interface for editing the cm\_kms service. The top navigation bar includes links for Access Manager, Audit, Encryption, and Settings. The user is logged in as keyadmin. The 'Edit Service' page displays the following configuration options:

- Active Status:** Enabled (selected) or Disabled.
- Select Tag Service:** A dropdown menu showing 'Select Tag Service'.
- Config Properties:**
  - KMS URL \*:** jhoyier.rangerkms-3.djhoyier.rangerkms.root.hwx.site:9292/kms
  - Username \*:** keyadmin
  - Password \*:** Masked with dots.
- Add New Configurations:** A table with columns 'Name' and 'Value'.
 

Name	Value
policy.download.auth.users	keyadmin,rangerkms

 A '+' button is available to add more configurations.
- Buttons:** Test Connection, Save, Cancel, and Delete.

**10.** In Cloudera Manager, select Ranger KMS with Key Trustee Server, then click Configuration.

a) Use the Add (+) icons for the Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kms-site.xml property to add the following properties, then click Save Changes.

- `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <Zookeeper hostname>:2181`



**Note:** Set this property only to override the default value.

- `hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = <provide a znode working path other than /zkdt-sm to avoid collision>`

For example:

`hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = testzkms`



**Note:** Do not put a leading slash at the beginning of the znode working path. Set this property only to override the default value.

- `hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType = sasl`



**Note:** Default value is *none* and it will give all the permission to the default node created in ZK. So, the recommended setting is *sasl*. If set to *sasl*, for example, the ACL at custom /zk path is:  
`'sasl','HTTP:cdrwa`

- `hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab = {{CMF_CONF_DIR}}/ranger_kms_kts.keytab`



**Important:** If you set *sasl* (as recommended) for `hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType`, then you must set `hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab = {{CMF_CONF_DIR}}/ranger_kms_kts.keytab`.

---

20

11. Update the following Ranger KMS configuration properties, then click Save Changes.

- `hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type = sasl`

For example, select `sasl` in the Ranger KMS Server with KTS Default Group.

The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the Configuration page for the service RANGER\_KMS\_KTS-1. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area displays a search bar with the query 'hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type'. Below the search bar, there are filters for SCOPE, CATEGORY, and STATUS. The SCOPE filter shows 'RANGER\_KMS\_KTS-1 (Service...)' with 0 results and 'Ranger KMS Server with KTS' with 1 result. The CATEGORY filter shows various categories like Advanced, Logs, Main, Monitoring, Performance, Ports and Addresses, Resource Management, Security, and Stacks Collection, all with 0 results. The STATUS filter shows Error (0), Warning (0), Edited (1), Non-default (1), and Has Overrides (0). The main configuration table shows the property 'hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type' with a value of 'sasl'. The 'Save Changes (CTRL+S)' button is visible at the bottom right.

12. Click the Stale Configuration Restart icon.

The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the Configuration page for the service RANGER\_KMS\_KTS-1. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area displays a search bar with the query 'hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type'. Below the search bar, there are filters for SCOPE, CATEGORY, and STATUS. The SCOPE filter shows 'RANGER\_KMS\_KTS-1 (Service...)' with 0 results and 'Ranger KMS Server with KTS' with 1 result. The CATEGORY filter shows various categories like Advanced, Logs, Main, Monitoring, Performance, Ports and Addresses, Resource Management, Security, and Stacks Collection, all with 0 results. The STATUS filter shows Error (0), Warning (0), Edited (0), Non-default (1), and Has Overrides (0). The main configuration table shows the property 'hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type' with a value of 'sasl'. A 'Stale Configuration Restart needed' icon is highlighted in the top right corner. The 'Save Changes (CTRL+S)' button is visible at the bottom right.

13. On the Stale Configurations page, click Restart Stale Services.

14. On the Restart Stale Services page, select the Re-deploy client configuration checkbox, then click Restart Now.

15. A progress indicator page appears while the services are being restarted. When the services have restarted, click Finish.